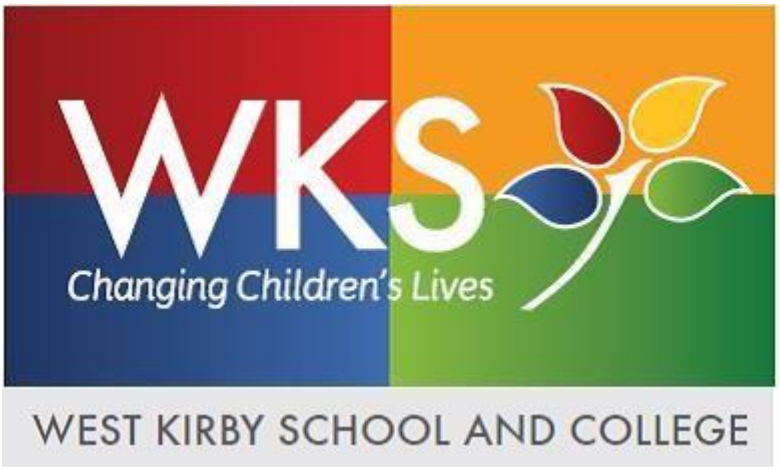


West Kirby School and College

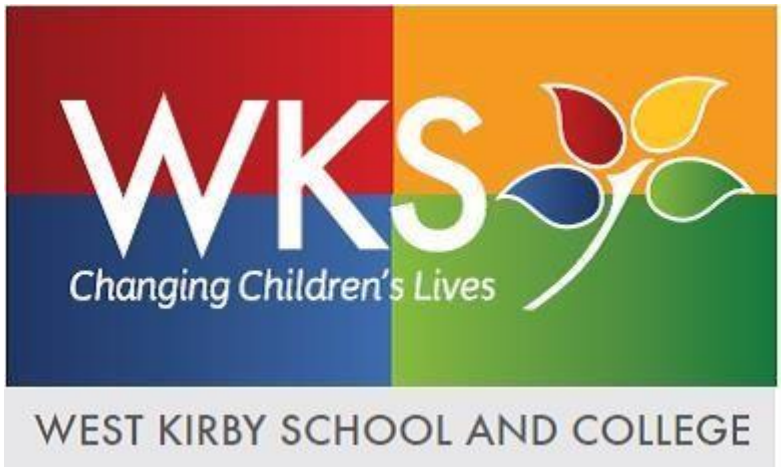
Data Protection & Information Security Handbook

June 2021

Written by:	Luke Cowell	**Date:**	June 2021
Last reviewed on:	June 2021		

DATA PROTECTION & INFORMATION SECURITY HANDBOOK
PROCEDURES AND POLICIES

CONTENTS



West Kirby School and College

Data Protection Policy

June 2021

Written By:	Luke Cowell	**Date:** June 2021	
Last reviewed on:	June 2021		

Contents:

Statement of intent

West Kirby School & College is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the GDPR.

The School may, from time to time, be required to share personal information about its staff or pupils with other organisations, other Schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff, governors and trustees are aware of their responsibilities and outlines how the School complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and West Kirby School & College believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation
    - The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
    - The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
        - The School Standards and Framework Act 1998
        - The Data Protection Act 2018

1.2. This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'
- DfE (2018) 'Data protection: a toolkit for Schools'

1.3. This policy will be implemented in conjunction with the following other School policies:

- Photography and Videos at School Policy
- Data and E-security Breach Prevention and Management Policy
- Surveillance & CCTV Policy
- Child Protection and Safeguarding Policy
- Records Management Policy

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those that were in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

4. Accountability

4.1. West Kirby School & College will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The School will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.

- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

4.5. The School will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.6. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to:

- Inform and advise the School and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the School's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to Schools.

5.4. The DPO will report to the highest level of management at the School, which is the Principal.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:

— Compliance with a legal obligation.
— The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
— For the performance of a contract with the data subject or to take steps to enter into a contract.
— Protecting the vital interests of a data subject or another person.
— For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the School in the performance of its tasks.)

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:

— Carrying out obligations under employment, social security or social protection law, or a collective agreement.
— Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
— The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

6.4. Where the School relies on:

- 'Performance of contract' to process a child's data, the School considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the School takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the School ensures that the requirements outlined in 7.7 and 7.8 are met, and the School does not exploit any imbalance of power in the relationship between the School and the child.

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The School ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. Where the School opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined in 7.2, the School obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

7.8. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the School on a case-by-case basis, taking into account the requirements outlined in 7.2.

8. Sharing data without consent

8.1. The School may share information without consent in specific circumstances. To determine whether information can be shared with consent, the School will identify one of the other lawful bases for processing:

- **Contract** – the processing is necessary for a contract held between the School and individual, or because the individual has asked the School to take specific tests before entering into a contract.
- **Legal obligation** – the processing is necessary for the School to comply with the law (not including contractual obligations).
- **Vital interests** – the processing is necessary to protect someone's life.
- **Public task** – the processing is necessary for the School to perform a task in the public interest or for it's official functions, and the task or function has a clear basis in law.
- **Legitimate interests** – the processing is necessary for the School's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.

8.2. Where the School is able to justify one of the lawful bases outlined in 8.1, an exemption applies, or there is a requirement under another law, information may be shared without consent.

8.3. Specifically, the GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

9. The right to be informed

9.1. Adults and children have the same right to be informed about how the School uses their data.

9.2. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

9.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:

— Withdraw consent at any time.

— Lodge a complaint with a supervisory authority.

- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

9.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

9.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the School holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

9.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

9.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access

10.1. Individuals, including children, have the right to obtain confirmation that their data is being processed.

10.2. Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

10.3. The School will verify the identity of the person making the request before any information is supplied.

10.4. A copy of the information will be supplied to the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for further copies of the same information.

10.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.7. All fees will be based on the administrative cost of providing the information.

10.8. All requests will be responded to without delay and at the latest, within one month of receipt.

10.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

10.10. Where a request is manifestly unfounded or excessive, the School holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.11. In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.

11. The right to rectification

11.1. Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

11.2. Where the personal data in question has been disclosed to third parties, the School will inform them of the rectification where possible.

11.3. Where appropriate, the School will inform the individual about the third parties that the data has been disclosed to.

11.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

11.5. Where no action is being taken in response to a request for rectification, the School will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

12.1. Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

12.2. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

12.3. The School has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

12.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.6. Where personal data has been made public within an online environment, the School will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

13.1. Individuals, including children, have the right to block or suppress the School's processing of personal data.

13.2. In the event that processing is restricted, the School will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.3. The School will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the School has verified the accuracy of the data
- Where an individual has objected to the processing and the School is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the School no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4. If the personal data in question has been disclosed to third parties, the School will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.5. The School will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

14.1. Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services.

14.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

14.4. Personal data will be provided in a structured, commonly used and machine-readable form.

14.5. The School will provide the information free of charge.

14.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7. The School is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8. In the event that the personal data concerns more than one individual, the School will consider whether providing the information would prejudice the rights of any other individual.

14.9. The School will respond to any requests for portability within one month.

14.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

14.11. Where no action is being taken in response to a request, the School will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

15.1. The School will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

15.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The School will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the School can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4. Where personal data is processed for direct marketing purposes:

- The School will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The School cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the School is not required to comply with an objection to the processing of the data.

15.6. Where the processing activity is outlined above, but is carried out online, the School will offer a method for individuals to object online.

16. Automated decision making and profiling

16.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2. The School will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3. When automatically processing personal data for profiling purposes, the School will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The School has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments

17.1. The School will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the School has considered and integrated data protection into processing activities.

17.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the School's data protection obligations and meeting individuals' expectations of privacy.

17.3. DPIAs will allow the School to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the School's reputation which might otherwise occur.

17.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5. A DPIA will be used for more than one project, where necessary.

17.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

17.7. The School will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

17.8. Where a DPIA indicates high risk data processing, the School will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

18. Data breaches

18.1. The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2. The DPO will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the School becoming aware of it.

18.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

18.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the School will notify those concerned directly.

18.7. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the School, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

19.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

19.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

19.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

19.6. All electronic devices are password-protected to protect the information on the device in case of theft.

19.7. Where possible, the School enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.8. Staff and governors will not use their personal laptops or computers for School purposes.

19.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

19.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

19.13. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the School premises accepts full responsibility for the security of the data.

19.14. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

19.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the School containing sensitive information are supervised at all times.

19.16. The physical security of the School's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

19.17. West Kirby School & College takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.18. The Operations Director is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

20.1. West Kirby School & College will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.2. When uploading information to the School website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

21.1. The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2. The School notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

21.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4. All CCTV footage will be kept for 30 days for security purposes; the Compliance Manager is responsible for keeping the records secure and allowing access.

21.5. The School will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

21.6. If the School wishes to use images/video footage of pupils in a publication, such as the School website, prospectus, or recordings of School plays, written permission will be sought for the particular usage from the parent of the pupil.

21.7. Precautions, as outlined in the Photography and Videos at School Policy, are taken when publishing photographs of pupils, in print, video or on the School website.

21.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

22. Data retention

22.1. Data will not be kept for longer than is necessary.

22.2. Unrequired data will be deleted as soon as practicable.

22.3. Some educational records relating to former pupils or employees of the School may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

23. DBS data

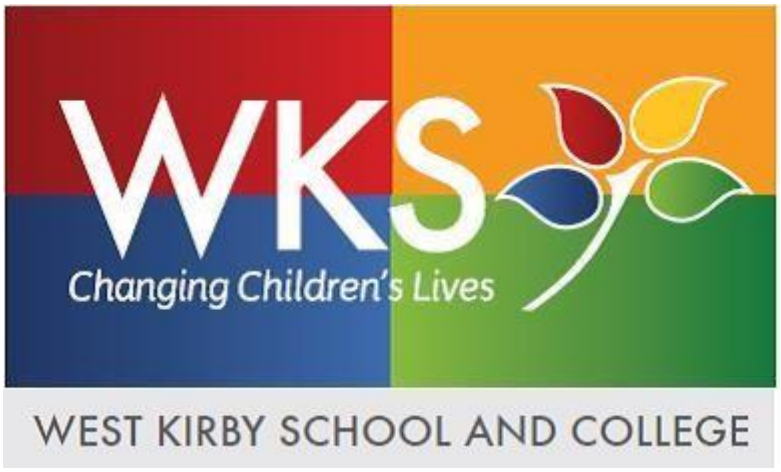
23.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2. Data provided by the DBS will never be duplicated.

23.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Policy review

24.1. This policy is reviewed every two years by the DPO, Operations Director and the Principal (overseen by a member of the Trustee Body).


WKS
Changing Children's Lives
WEST KIRBY SCHOOL AND COLLEGE

West Kirby School and College

Data and E-Security Breach Prevention Policy & Plan November 2020

Written by:	Luke Cowell	Date:	November 2020
Last reviewed on:	November 2020		

Contents:

14. Assessment of risks
15. Consideration of further notification
16. Evaluation and response
17. Monitoring and review

Appendix:

a) Timeline of Incident Management

Statement of intent

West Kirby School & College is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the School are only accessible by the appropriate individuals. It is, therefore, important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The School recognises, however, that breaches in security can occur, particularly as most information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence.

1. Legal framework

1.1. This policy has due regard to statutory legislation and advisory guidance including, but not limited to, the following:

- The Computer Misuse Act 1990
- The General Data Protection Regulation (GDPR)
- National Cyber Security Centre (2018) 'Cyber Security: Small Business Guide'

1.2. This policy has due regard to the School's policies and procedures including, but not limited to, the following:

- Data Protection Policy

2. Types of security breach and causes

2.1. **Unauthorised use without damage to data** – involves unauthorised persons accessing data on the School system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

2.2. **Unauthorised removal of data** – involves an authorised person accessing data, who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

2.3. **Damage to physical systems** – involves damage to the hardware in the School's ICT system, which may result in data being inaccessible to the School and/or becoming accessible to unauthorised persons.

2.4. **Unauthorised damage to data** – involves an unauthorised person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

2.5. Breaches in security may be caused as a result of actions by individuals, which may be accidental, malicious or the result of negligence – these can include:

- Accidental breaches, e.g. as a result of insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the School through accessing and altering, sharing or removing data.

- Negligence, e.g. as a result of an employee that is aware of School policies and procedures, but disregards these.

2.6. Breaches in security may also be caused as a result of system issues, which could involve incorrect installation, configuration problems or an operational error – these can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the School software is more vulnerable to a virus
- Incorrect firewall settings are applied, e.g. access to the School network, meaning individuals other than those required could access the system
- Confusion between backup copies of data, meaning the most recent data could be overwritten

2.7. Security breaches as a result of employee action or inaction (howsoever they may occur), may be dealt with under the School's Disciplinary Policy.

3. Roles and responsibilities

3.1. The Data Protection Officer (DPO) is responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use, and for keeping the School's network services, data and users safe, in conjunction with the Operations Director.
- Leading on the School's response to incidents of data security breaches.
- Assessing the risks to the School in the event of a data security breach.
- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Working with the Operations Director and Principal after a data security breach to determine where weaknesses lie and improve security measures.
- Organising training for staff members on data security and preventing breaches.
- Monitoring the effectiveness of this policy, alongside the Operations Director and Principal, and communicating any changes to staff members.

3.2. The IT Manager is responsible for:

- Maintaining an inventory of all ICT hardware and software currently in use at the School.
- Ensuring any software that is out-of-date is removed from the School premises.
- Implementing effective firewalls to enhance network security and ensuring that these are monitored regularly.
- Ensuring all School-owned devices have secure malware protection and that devices are regularly updated.
- Installing, monitoring and reviewing filtering systems for the School's network.
- Setting up user privileges in line with recommendations from the Operations Director and Principal.
- Maintaining an up-to-date inventory of all usernames and passwords.
- Removing any inactive users from the School's system, ensuring that this is always up-to-date.
- Recording any alerts for access to inappropriate content and notifying the Operations Director and Principal.
- Installing appropriate security software on staff members' personal devices where the Operations Director or Principal has permitted for them to be used for work purposes.
- Performing a back-up of all electronic data held by the School, ensuring detailed records of findings are kept.
- Organising training for staff members on network security.

3.3. The Operations Director and Principal are responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Defining users' access rights for both staff and pupils, communicating these to the IT Manager and maintaining a written record of privileges.
- Informing the IT Manager of staff members who are permitted to use their personal devices for work purposes so that appropriate security methods can be applied.
- Issuing disciplinary sanctions to pupils or members of staff who cause a data security breach.
- Organising training for staff members in conjunction with the IT Manager and DPO.

4. Secure configuration

4.1. An inventory will be kept of all ICT hardware and software currently in use at the School, including mobile phones and other personal devices provided by the School. This will be stored in the IT office and will be audited on a periodical basis to ensure it is up-to-date.

4.2. Any changes to the ICT hardware or software will be documented using the inventory and will be authorised by the IT Manager before use.

4.3. All systems will be audited on a periodical basis by the IT Manager to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded in the inventory.

4.4. Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

4.5. All hardware, software and operating systems will require passwords from individual users before use. Passwords will be changed on a periodical basis to prevent access to facilities which could compromise network security.

4.6. The School believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users.

5. Network security

5.1. The School will employ firewalls in order to prevent unauthorised access to the systems.

5.2. The School's firewall will be deployed as a:

- Localised deployment: the broadband service connects to a firewall that is located on an appliance or system on the School premises, as either discrete technology or a component of another system.

5.3. As the School's firewall is managed on the premises, it is the responsibility of the IT Manager to effectively manage the firewall. The IT Manager will ensure that:

- The firewall is checked monthly for any changes and/or updates, and that these are recorded using the inventory.

- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is checked monthly to ensure that a high level of security is maintained and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the DPO and Operations Director. The IT Manager will react to security threats to find new ways of managing the firewall.

6. Malware prevention

6.1. The School understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

6.2. The IT Manager will ensure that all School devices have secure malware protection and undergo regular malware scans in line with specific requirements.

6.3. The IT Manager will update malware protection on a regular basis to ensure it is up-to-date and can react to changing threats.

6.4. Malware protection will also be updated in the event of any attacks to the School's hardware and software.

6.5. Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware are blocked immediately and reported to IT Manager.

6.6. The School will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

6.7. The IT Manager will review the mail security technology on a regular basis to ensure it is kept up-to-date and effective.

6.8. Staff members are only permitted to download apps on any School-owned device from manufacturer-approved stores and with prior approval from the IT Manager or Operations Director.

6.9. Where apps are installed, the IT Manager will keep up-to-date with any updates, ensuring staff are informed of when updates are ready, how to install them, and that they should do this without delay.

7. User privileges

7.1. The School understands that controlling what users have access to is important for promoting network security. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

7.2. The Operations Director and Principal will clearly define what users have access to and will communicate this to the IT Manager, ensuring that a written record is kept.

7.3. The IT Manager will ensure that user accounts are set up to allow users access to the facilities required, in line with the Operations Director's or Principal's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

7.4. The IT Manager will ensure that websites are filtered on an ongoing basis for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 13 of this policy.

7.5. All users will be required to change their passwords on a periodical basis and will use upper and lowercase letters, as well as numbers, to ensure that passwords are strong.

7.6. Users will also be required to change their password if they become known to other individuals.

7.7. Pupils are responsible for remembering their passwords; however, the IT Manager will have an up-to-date record of all usernames and passwords and will be able to reset them if necessary.

7.8. The record of all usernames and passwords is encrypted. Only the IT Manager has access to this inventory.

7.9. The 'master user' password used by the IT Manager will be made available to the Operations Director, Principal, DPO and any other nominated senior leader, and will be kept in the Operations Director's safe.

7.10. The master user account accessed by the IT Manager, DPO, Operations Director and Principal is subject to a two-factor authentication for logins. This account requires two different methods to provide identity before logging in – these are:

7.10.1. A password; and a

7.10.2. Code sent to another School-owned device, such as a tablet, which must be entered following the password.

7.11. The master user account is used as the 'administrator' which allows designated users to make changes that will affect other users' accounts in the School, such as changing security settings, monitoring use, and installing software and hardware.

7.12. A multi-user account will be created for visitors to the School, such as volunteers, and access will be filtered as per the Operations Director's or Principal's instructions. Usernames and passwords for this account will be changed on a periodical basis and will be provided as required.

7.13. Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the School. The IT Manager will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

7.14. The IT Manager will review the system on a periodical basis to ensure the system is working at the required level.

8. Monitoring usage

8.1. Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff.

8.2. The School will inform all pupils and staff that their usage will be monitored, in accordance with the School's other IT policies.

8.3. If a user accesses inappropriate content or a threat is detected, an alert will be sent to the IT Manager. Alerts will also be sent for unauthorised and accidental usage.

8.4. Alerts will identify: the user, the activity that prompted the alert and the information or service the user was attempting to access.

8.5. The IT Manager will record any alerts using an incident log and will report this to the Principal and Operations Director. All incidents will be responded to in accordance with section 13 of this policy.

9. Removable media controls and home working

9.1. The School understands that pupils and staff may need to access the School network from areas other than on the premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

9.2. The IT Manager will encrypt all School-owned devices, such as laptops, mobile phones and tablets, to ensure that they are password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

9.3. Before distributing any School-owned devices, the IT Manager will ensure that manufactures' default passwords have been changed. A set password will be chosen and the staff member will be prompted to change the password once using the device.

9.4. The IT Manager will check School-owned devices on a periodical basis to detect any unchanged default passwords.

9.5. Staff are not permitted to use their personal devices for work purposes under ANY circumstances, such as personal laptops, personal computers, tablets, mobile phones and USB sticks. Staff who contravene this strict policy will be liable to disciplinary action (up to and including dismissal).

9.6. When using laptops, tablets and other portable devices, the Principal will determine the limitations for access to the network, as described in section 5 of this policy.

9.7. Staff who use School-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the School premises.

9.8. Staff members will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any laptops, tablets or other devices.

9.9. The IT Manager will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

9.10. The School uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.

9.11. All data will be held on systems centrally in order to reduce the need for the creation of multiple copies, and/or the need to transfer data using removable media controls.

9.12. The Wi-Fi network at the School will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Operations Director or Principal.

9.13. A separate Wi-Fi network will be established for visitors at the School to limit their access to printers, shared storage areas and any other applications which are not necessary.

10. Backing-up data

10.1. The IT Manager performs a back-up of all electronic data held by the School on a periodical basis.

10.2. Where possible, back-ups are run overnight and are completed before the beginning of the next School day.

10.3. Upon completion of back-ups, data is stored on the School's hardware which is password protected.

10.4. Only authorised personnel are able to access the School's data.

11. Avoiding phishing attacks

11.1. The IT Manager will configure all staff accounts using the principle of 'least privilege' – staff members are only provided with as much rights as are required to perform their jobs.

11.2. Designated individuals who have access to the master user account will avoid browsing the web or checking emails whilst using this account.

11.3. Two-factor authentication is used on any important accounts, such as the master user account.

11.4. In accordance with section 12 of this policy, the IT Manager, Operations Director and Principal will organise regular training for staff members – this will cover identifying irregular emails in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual.

11.5. Staff will use the following warning signs when considering whether an email may be unusual:

- Is the email from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is the email addressed to a 'valued customer', 'friend' or 'colleague'?
- Does the email contain a veiled threat that asks the staff member to act urgently?
- Is the email from a senior member of the School asking for a payment?

- Does the email sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.

11.6. The IT Manager will ensure that email filtering systems, applied in accordance with section 6 of this policy, are neither too strict or lenient; filtering that is too strict may lead to legitimate emails becoming lost, and too lenient filters may mean that emails that are spam or junk are not sent to the relevant folder.

11.7. To prevent hackers having access to unnecessary public information, the DPO will ensure the School's social media accounts and websites are reviewed on a periodical basis, making sure that only necessary information is shared.

12. User training and awareness

12.1. The IT Manager, Operations Director and Principal will arrange training for pupils and staff on a periodical basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy.

12.2. The DPO will also arrange training for pupils and staff on a periodical basis maintaining data security, preventing data breaches, and how to respond in the event of a data breach.

12.3. Training for all staff members will be arranged by the IT Manager and DPO within two weeks following an attack, breach or significant update.

12.4. Through training, all pupils and staff will be aware of who they should inform first in the event that they suspect a security breach, and who they should inform if they suspect someone else is using their passwords.

12.5. All staff will receive training as part of their induction programme, as well as any new pupils who join the School.

12.6. All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks.

13. Security breach incidents

13.1. Any individual that discovers a security data breach will report this <u>immediately</u> (by phone) to:

1. **The DPO - 07308 596 810.** If the DPO is unreachable, then call;

2. **The Operations Director – 07308 601 122**. If the Operations Director is unreachable, then call;

3. **The Principal – 07308 599 593**. If the Principal is unreachable move back to step 1 and continue to call until you can speak to someone to report the security data breach.

Either the DPO, Operations Director or the Principal will inform the IT Manager.

- After reporting the incident verbally, the individual that discovers the security data breach must fill in the data breach reporting form **within 30 minutes** of ending the call with the person that they have reported the security data breach to. The data breach reporting form (**Appendix B**) must then be emailed to databreach@wkrs.co.uk. The data breach reporting form is available to download from the School's 'Every Management System'.

- When an incident is raised, the DPO (or Operation Director or Principal in their absence) will ensure the data breach reporting form contains the following key (and mandatory) information:

    a) Name of the individual who has raised the incident

    b) Description and date of the incident

    c) Description of any perceived impact

    d) Description and identification codes of any devices involved, e.g. School-owned laptop

    e) Location of the equipment involved

    f) If there has been a delay in reporting the incident please explain the reasons for this

- The School's DPO (or Operation Director or Principal in their absence) will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

- The DPO (or Operation Director or Principal in their absence), as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or has been compromised.

- The DPO (or Operation Director or Principal in their absence) will (without delay) consult with the School's Data Protection Consultants (Judicium Education) for advice on how to manage the breach (and will fully act and comply upon that advice). **Judicium can be contacted on 020 3326 9174.** The DPO (or Operation Director or Principal in their absence) will get Judicium's advice confirmed in writing and will included that written advice (as evidence) with their report.

- The DPO (or Operation Director or Principal in their absence) will oversee a full investigation and produce a comprehensive report.
- The cause of the breach, and whether or not it has been contained, will be identified – ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.
- If the DPO (or Operation Director or Principal in their absence) determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:
    - In the event of an internal breach, the incident is recorded using an incident log (**Appendix A**), and by identifying the user and the website or service they were trying to access. The DPO is ultimately responsible for the accurate maintenance and secure storage of the incident log for the School.
    - The Operations Director or Principal will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the School's IT policies.
    - In the event of any external or internal breach, the DPO (or Operation Director or Principal in their absence) will record this using an incident log and respond appropriately, e.g. by updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information.
    - Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.
- Where the security risk is high, the DPO (or Operation Director or Principal in their absence) will establish which steps need to be taken to prevent further data loss which will require support from various School departments and staff. This action will include:
    - Informing relevant staff of their roles and responsibilities in areas of the containment process.
    - Taking systems offline.
    - Retrieving any lost, stolen or otherwise unaccounted for data.
    - Restricting access to systems entirely or to a small group.
    - Backing up all existing data and storing it in a safe location.
    - Reviewing basic security, including:
        - Changing passwords and login details on electronic equipment.
        - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

- Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO (or Operation Director or Principal in their absence) will inform the police of the security breach.
- Where the School has been subject to online fraud, scams or extortion the DPO (or Operation Director or Principal in their absence) will also report this using the Action Fraud website.
- The IT Manager will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the School's systems are safe to use.

14. Assessment of risks

- The following questions will be considered by the DPO (or Operation Director or Principal in their absence) to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the School's report and records:
    - What type and how much data is involved?
    - How sensitive is the data? Sensitive data is defined in the GDPR; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
    - Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
    - If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?
    - If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
    - Has individuals' personal data been compromised – how many individuals are affected?
    - Who are these individuals – are they pupils, staff, governors, volunteers, stakeholders, suppliers?
    - Could their information be misused or manipulated in any way?

- Could harm come to individuals? This could include risks to the following:
    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public

- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the School's reputation, or risk to the School's operations?

- Who could help or advise the School on the breach?

- In the event that the DPO (or Operation Director or Principal in their absence), or other persons involved in assessing the risks to the School, are not confident in the risk assessment, they will seek advice from the ICO.

15. Consideration of further notification

- The DPO (or Operation Director or Principal in their absence) will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security (see 15.8 onwards for specific GDPR requirements about personal data).

- The DPO (or Operation Director or Principal in their absence) will assess whether notification could help the individual(s) affected, and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

- If a large number of people are affected, or there are very serious consequences, the ICO will be informed.

- The DPO (or Operation Director or Principal in their absence) will consider who to notify, what to tell them and how they will communicate the message, which may include:

    - A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.

- Specific and clear advice on the steps they can take to protect themselves, and what the School is willing to do to help them.
- A way in which they can contact the School for further information or to ask questions about what has occurred.

- The ICO will be consulted for guidance on when and how to notify them about breaches.
- The DPO (or Operation Director or Principal in their absence) will consider, as necessary, the need to notify any third parties – police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.
- The DPO (or Operation Director or Principal in their absence) will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.
- Where a breach is likely to result in a significant risk to the rights and freedoms of individuals, the DPO (or Operation Director or Principal in their absence) will notify those concerned directly of the breach.
- Where the breach compromises personal information, the notification will contain:
    - The nature of the personal data breach including, where possible:
        - The type(s), e.g. staff, pupils or governors, and approximate number of individuals concerned.
        - The type(s) and approximate number of personal data records concerned.
    - The name and contact details of the DPO or other person(s) responsible for handling the School's information.
    - A description of the likely consequences of the personal data breach.
    - A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

16. Evaluation and response

- The DPO (or Operation Director or Principal in their absence) will establish the root of the breach, and where any present or future risks lie.

- The DPO (or Operation Director or Principal in their absence) will consider the data and contexts involved.
- The DPO (or Operation Director or Principal in their absence) will identify any weak points in existing security measures and procedures.
- The DPO (or Operation Director or Principal in their absence) will work with the IT Manager to improve security procedures wherever required.
- The DPO (or Operation Director or Principal in their absence) will identify any weak points in levels of security awareness and training.
- The DPO (or Operation Director or Principal in their absence) will report on findings and, with the approval of the School leadership team, implement the recommendations of the report after analysis and discussion.

17. Monitoring and review

- This policy will be reviewed by the Operations Director and Principal, in conjunction with the DPO and IT Manager, on a periodical basis.
- The DPO is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members

Data Breach Incident Log

(Appendix B)

Date of breach	Time of breach	Activity	Decision	Name/position investigating breach	Date breach investigated

Data Protection Breach Reporting

(Appendix B)

INSTRUCTIONS FOR USE:

Any individual that discovers a security data breach will report this immediately (by phone) to:

- **The DPO - 07308 596 810.** If the DPO is unreachable, then call;
- **The Operations Director – 07308 601 122**. If the Operations Director is unreachable, then call;
- **The Principal – 07308 599 593**. If the Principal is unreachable move back to step 1 and continue to call until you can speak to someone to report the security data breach.

After reporting the incident verbally, complete this form **within 30 minutes** of ending the call with the person that you have reported the security data breach to. The form must then be immediately emailed to databreach@wkrs.co.uk.

Please describe the incident in as much detail as possible.

DATA BREACH REPORTING FORM

Individual who is reporting the breach complete sections highlighted in yellow

DPO (Or Operations Director or Principal in their absence) complete sections highlighted in green

Incident Summary

a) Name of Individual reporting this incident
b) When did the incident happen (date and time)?
c) Description of the incident
d) *How did the incident happen?*

e) Description of any perceived impact
f) Description and identification codes of any devices involved, e.g. School-owned laptop
g) Location of the equipment involved
h) If there has been a delay in reporting the incident please explain the reasons for this.
i) What measures were in place to prevent an incident of this nature occurring?
j) Please provide extracts from any policies or procedures considered relevant to this incident, and explain which of these were in existence at the time of this incident. Please provide the dates on which they were implemented.

Personal data placed at risk

k) What personal data has been placed at risk? Please specify if any financial or sensitive personal data (special categories) has been affected and provide details of the extent.*
l) How many individuals have been affected and how many data records are involved?
m) Are the affected individuals aware that the incident has occurred?
n) What are the potential consequences and adverse effects on those individuals?
o) Have any affected individuals complained to the School about the incident?

Containment and recovery

p) Has any action been taken to minimise/mitigate the effect on the affected individuals? If so, please provide details.

q) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
r) What steps have been taken to prevent a recurrence of this incident?

Miscellaneous

s) Have the police or any other regulatory bodies been informed about this incident?
t) Has there been any media coverage of the incident?

Management Records

u) Who has managed this incident at the School (name and job title) i.e DPO – Pete Smith?
v) What date and time was the incident closed?
w) Has the incident log been updated to reflect and contain full and accurate details of this incident?

NB: Judicium's written advice on how to manage this situation must be stored along with this completed form (see page 38 of this Policy).

West Kirby School and College

Confidentiality Policy (For Staff, Volunteers, Trustees and Governors) June 2021

Written by:	Luke Cowell	Date: June 2021	
Last reviewed on:	June 2021		

Contents:

Statement of intent

This document guides staff, volunteers and visitors on the policy and procedures surrounding confidentiality.

Staff members take a supportive and accepting attitude towards pupils as part of their general responsibility for pastoral care. It is our hope that both pupils and parents feel free to discuss worries about West Kirby School & College, and concerns that may affect the educational progress of a pupil, with members of the School team.

This policy will be abided by at all times by staff, volunteers, visitors, pupils and parents. In order to ensure the utmost level of safety for pupils, staff members at the School have a duty to act in accordance with this policy and not share information with external agencies, other Schools or individuals.

The Staff and Volunteer Confidentiality Policy has the following benefits, it:

- Ensures that important information regarding the School is not shared.
- Guarantees that financial information stays confidential and secure.
- Helps to build trust amongst staff, volunteers and external agencies.
- Supports the School's safeguarding measures.

1. Legal framework

1.1. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Crime and Disorder Act 1998
- Equality Act 2010
- The General Data Protection Regulation
- Data Protection Act 2018
- Education Act 2002
- Human Rights Act 1998
- The Education (Pupil Information) (England) (Amendment) Regulations 2019 This policy is compliant under the following case law:
- The Common Law Duty of Confidentiality

1.2. This policy also has due regard to guidance documents including, but not limited to, the following:

- DfE (2018) 'Information sharing'
- DfE (2018) 'Working Together to Safeguard Children'

1.3. This policy operates in conjunction with the following School policies:

- Data Protection Policy
- Records Management Policy
- Child Protection and Safeguarding Policy
- Anti-bullying Policy
- Whistleblowing Policy
- E-safety Policy

2. Definitions

2.1. For the purpose of this policy, '**confidentiality**' is an understanding that any information shared with someone in trust will only be passed on to a third party with the prior and explicit agreement of the person disclosing it.

2.2. Within this policy, a 'disclosure' is the sharing of any private information; this term does not solely relate to child protection issues.

2.3. The term ‘limited confidentiality’ refers to the disclosure of information with professional colleagues; however, the confider would not be identified except in pre-determined circumstances.

3. Roles and responsibilities

3.1. All staff members, volunteers and individuals working in cooperation with the School will uphold their responsibility and duty of confidentiality, ensuring that information and personal details are not shared or discussed with others, except for the appropriate necessary bodies.

3.2. Visitors, volunteers and other professionals, such as healthcare professionals, will work within the same boundaries of confidentiality as all staff members.

3.3. Staff members and volunteers alike, have the responsibility of keeping information regarding the School, including its pupils and parents, etc., confidential. This information will under no circumstances be shared, unless it is in the best interest of the School or its pupils.

3.4. All staff members, volunteers and external agencies will treat any information regarding the management and finance of the School as confidential, and, therefore, this information will only be shared with necessary and appropriate external individuals.

3.5. Members of staff, volunteers, visitors, external parties and other agencies will always seek advice from a practitioner at the School if there is any doubt over sharing the information concerned, without disclosing any identifiable information where possible.

3.6. As a precautionary safeguarding measure, the School may ask staff members, volunteers, visitors and external agencies who work closely with the School to sign a Non-disclosure Agreement.

3.7. The School will adopt a Nondisclosure Agreement, such as the example in Appendix B, to meet the needs of each circumstance. This means that information about the School which is shared with the individual is to be treated and not shared further.

3.8. The Principal and Operations Director are jointly responsible for ensuring that a confidentiality agreement is signed by all individuals who may be privy to information which is not suitable to be shared.

4. Confidentiality and child protection

4.1. The School aims to strike a balance between confidentiality and trust, ensuring the safety, wellbeing and protection of our pupils.

4.2. Staff members and volunteers alike will pass on information if they believe a child is at risk of harm, otherwise, staff are not obliged to break confidentiality.

4.3. In almost all cases of disclosure, limited confidentiality is able to be maintained.

4.4. Staff members and volunteers will use their professional judgement when considering whether to inform a child that a disclosure may be made in confidence and whether such confidence could remain having heard the information, bearing in mind that staff can never guarantee absolute confidentiality to pupils.

4.5. A member of the Safeguarding Team is to be informed of all incidents regarding child protection concerns which are highlighted by a volunteer, parent or another external party to the School.

4.6. Staff members are contractually obliged to immediately inform a member of the Safeguarding Team of any concerns regarding a pupil's safety or welfare.

4.7. Any concerns raised over a child's welfare and safety will be reported immediately to ensure that any intervention necessary to protect the child is accessed as early as possible.

4.8. Staff members are not obliged to inform the police on most matters relating to illegal activity, such as illegal drugs or assaults. These will be assessed on a case-by-case basis with the support of the SLT.

5. Sharing information

5.1. The School takes the stance that all information about individual pupils is private and should only be shared with other professionals who have a legitimate need to know.

5.2. Under no circumstances will personal information about pupils, staff members or the School be passed on indiscriminately.

5.3. Under no circumstances will information regarding the School's finances be shared with anyone, other than those with a legitimate need to know.

5.4. If members of staff, volunteers or cooperating external parties share unsuitable or misrepresented information, the School withholds the right to take the appropriate civil, legal or disciplinary action.

5.5. The safety and protection of pupils, as well as the School, is the paramount consideration in all confidentiality decisions.

5.6. All non-teaching staff and volunteers will report disclosures of a concerning personal nature to the DSL and DPO as soon as possible and in an appropriate setting.

5.7. All external visitors will be made aware of the Staff and Volunteer Confidentiality Policy and act in accordance with it when dealing with information, particularly sensitive information, regarding the School, its pupils and parents.

5.8. All data will be processed and held in line with the School's Data Protection Policy. In the event of information and data being shared with external or inappropriate parties, or electronic data being shared in an insecure way, the individual responsible will be liable for disciplinary or legal action in accordance with the Data Protection Policy.

5.9. The School will be open and honest with all individuals about how and why data is shared, unless it is unsafe to do so.

5.10. Where necessary, advice will be sought from the DPO and other practitioners to ensure all data is shared correctly.

5.11. Where possible, information is shared with consent from the data subject, unless the School is able to proceed without consent under the GDPR and Data Protection Act 2018, e.g. if the data subject's safety is at risk.

5.12. Individuals' safety and wellbeing will form the base of all information sharing decisions, and information will not be shared if anyone's safety or wellbeing could be compromised.

5.13. Only information that is necessary for the purpose it is being shared for will be shared.

5.14. All decisions and reasons for sharing data will be recorded by the DPO.

6. Breaking confidentiality

6.1. When confidentiality must be broken because a child may be at risk of harm, in accordance with the School's Child Protection and Safeguarding Policy, the School will ensure the following:

- Pupils are told when information has been passed on
- Pupils are kept informed about what will be done with their information

- To alleviate their fears concerning the information becoming common knowledge, pupils are told exactly who their information has been passed on to

6.2. If confidential information is shared with the explicit consent of the individuals involved, and they are informed of the purpose of sharing the information in question, there will be no breach of confidentiality or of the Human Rights Act 1998.

6.3. In the event that explicit consent for sharing confidential information is not gained, an individual will satisfy themselves that there are reasonable grounds to override the duty of confidentiality in these circumstances before sharing the data.

6.4. The School recognises that overriding public interest is a justifiable reason to disclose information; however, permission from the Principal or Operations Director will be sought prior to disclosing any information regarding the School.

6.5. Staff should act in accordance with the School's Whistleblowing Policy at all times.

6.6. Individuals who disclose information, after previously signing the School's confidentiality agreement, may face further action, including legal action.

6.7. Staff in breach of this policy may face disciplinary action, if it is deemed that confidential information was passed on to a third party without reasonable cause.

7. Accessing information

7.1. In accordance with article 15 of the GDPR, personal information, such as educational records, can be shared via a subject access request (SAR).

- These requests must be made in writing to the governing board and will be responded to within 15 School days if the request is regarding an educational record.
- If the data being requested is not in relation to an educational record, the response must be within one calendar month.
- Pupils, or the parent of a pupil, have the right to access the information that the School holds about the child in question.
- Some types of personal data are exempt from the right of a SAR and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have.
- Information regarding another individual must not be disclosed in a SAR.

- Individual requests for non-personal information cannot be treated as a SAR.

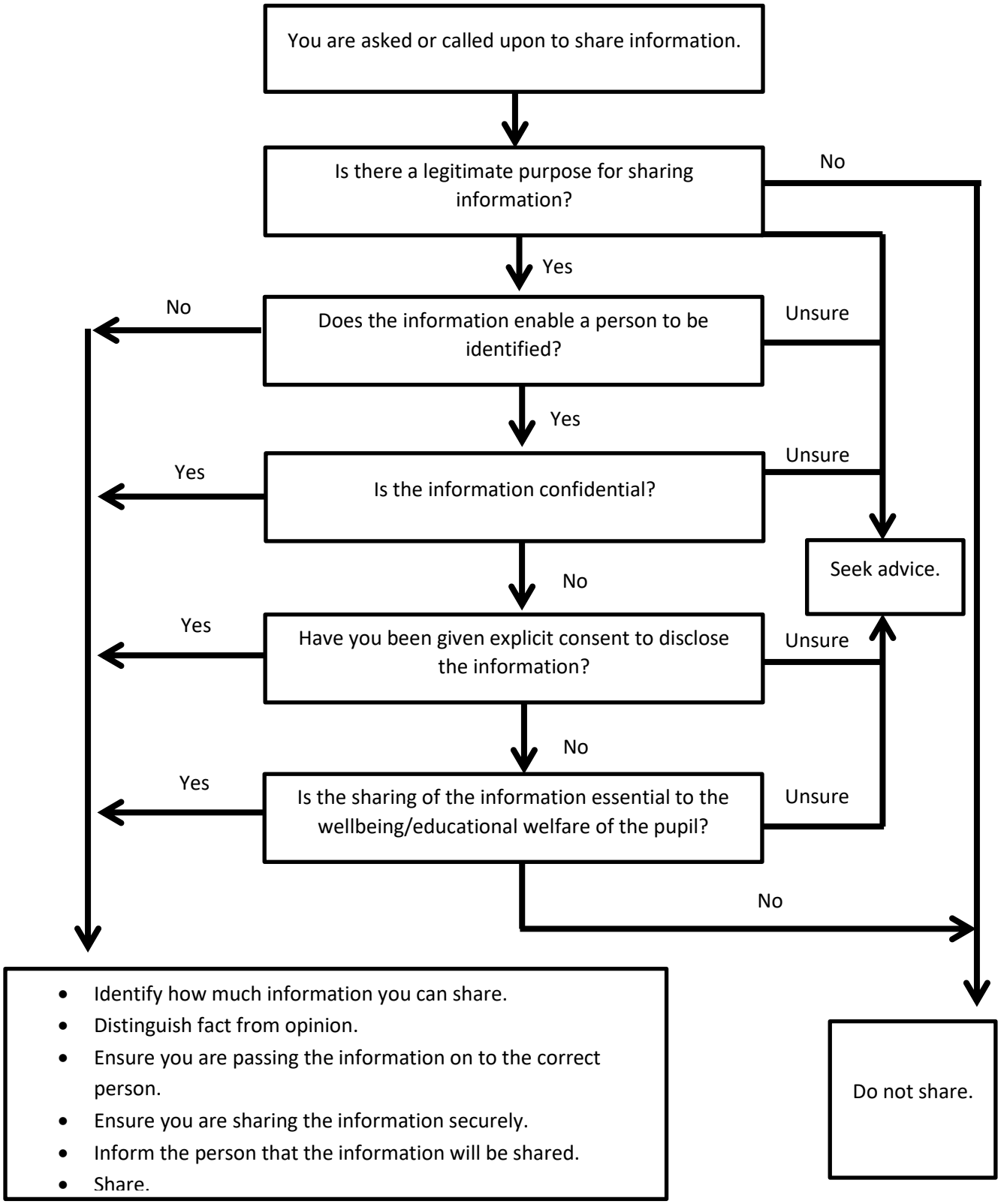
8. Monitoring and review

8.1. This policy is monitored for effectiveness by the Principal and Operations Director and is reviewed annually, or where necessary in light of changes to the law or statutory guidance.

8.2. A record of information which has been shared will be continuously kept up-to-date.

- This record will state the premise of the information, whom it was shared with and the purpose for sharing it.
- The record will be kept in the DPO's office and can be accessed by all appropriate staff members.
- On an annual basis, the Principal and DSL will review the record to ensure that all reasonable measures to safeguard pupils and protect the reputation of the School are being taken.

Appendix A – Information Sharing Flowchart



Notes

- If there are child protection concerns, follow the relevant procedures without delay.
- Always seek advice if you are unsure whether to share information.

Appendix B – Example Confidentiality Agreement

WEST KIRBY SCHOOL AND COLLEGE

This confidentiality agreement is entered into by and between West Kirby School & College and **name of individual**, **role within School**, for the purpose of preventing the unauthorised disclosure of confidential information in line with your duties to protect personal information under the Data Protection Act 2018.

For the purpose of this agreement, "confidential information" will include all information or material that has or could have value, commercial or otherwise, in the business in which the disclosing party is engaged.

I declare that, as a **role within School** of the School, I will only share or disclose information regarding the School with other professionals who have a legitimate need to know about it. I will, therefore:

- Not disclose confidential information to any unauthorised person without the discloser's consent.
- Act in good faith at all times in relation to the disclosure of confidential information.
- Not post confidential information regarding pupils, staff, parents or other stakeholders on social media. Nor will I contribute to discussions on social media regarding the School or anyone associated with it.
- Ensure that anything I hear that questions the professionalism of a member staff or volunteer of the School is reported to the Principal or Operations Director immediately.
- Ensure that if I notice anything of concern regarding the protection or safeguarding of a child, I will report it immediately to the Safeguarding Team.
- Assure that conversations of a sensitive nature regarding pupils, parents, staff, volunteers or other stakeholders take place in a private space.
- Comply with the School's Records Management Policy when completing tasks pertaining to paperwork or online documents that include personal or sensitive information.
- Be fully aware that other staff, volunteers or stakeholders may have connections within the School and may overhear conversations of a sensitive nature.
- Uphold the good name and reputation of the School at all times; inside and outside of School.

I will hold and maintain the confidential information in strictest confidence for the sole and exclusive benefit of the School; therefore, I will not, without prior approval of the School, use for my own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of the School, any confidential information.

I have read and understood the School's Confidentiality Policy and will act in accordance with this policy at all times.

Information which may be deemed as ‘sensitive’ will not be disclosed to people where it is not wholly necessary. This includes information in relation to the following:

- Pupils of the School
- The running or management of the School
- The School’s finances
- Personal details of pupils or staff
- Information regarding progress and attainment which is not published on the School website

By signing this agreement, you are agreeing to your duty to hold confidential information in confidence – this will remain in effect until the information no longer qualifies as confidential, or until the School sends written notice releasing you from this agreement, whichever occurs first.

Please retain a copy of this agreement and send a signed copy back to the School by **date**. If you have any questions or concerns, please contact the contact at the School who has issued you with this agreement to sign.

SIGNED BY (NAME): _____

ROLE: _____

SIGNATURE: _____

DATE: _____/_____/_____

Signed on Behalf of West Kirby School & College (below)

SIGNED BY (NAME): _____

POSITION IN SCHOOL: _____

SIGNATURE: _____

DATE: _____/_____/_____

West Kirby School and College

Surveillance and CCTV Policy June 2021

Written by:	Luke Cowell	Date: June 2021	
Last reviewed on:	June 2021		

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Purpose and justification
5. The data protection principles
6. Objectives
7. Protocols
8. Security
9. Privacy by design
10. Code of practice
11. Access
12. Monitoring and review

Statement of intent

At West Kirby School & College, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our School and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the School and ensure that:

- We comply with the GDPR, effective 25 May 2018.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

1. **Legal framework**

1.1. This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

1.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

1.3. This policy operates in conjunction with the following School policies:

- Photography and Videos at School Policy
- GDPR Data Protection Policy

2. Definitions

2.1. For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000.

- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

2.2. West Kirby School & College does not condone the use of covert surveillance when monitoring the School's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

2.3. Any overt surveillance footage will be clearly signposted around the School.

3. Roles and responsibilities

3.1. The role of the data protection officer (DPO) includes:

- Dealing with subject access requests (SAR) in line with legislation.
- Ensuring that all data controllers at the School handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the School, their rights for the data to be destroyed and the measures implemented by the School to protect individuals' personal information.
- Preparing reports and management information on the School's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the School, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the School's data protection impact assessment (DPIA) and providing advice where requested.

- Presenting reports regarding data processing at the School to senior leaders and the governing board.

3.2. West Kirby School & College, as the corporate body, is the data controller. The governing board of West Kirby School & College therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The DPO deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

3.4. The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

3.5. The role of the Principal (and/or Operations Director) includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the School is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

4. Purpose and justification

4.1. The School will only use surveillance cameras for the safety and security of the School and its staff, pupils and visitors.

4.2. Surveillance will be used as a deterrent for violent behaviour and damage to the School.

4.3. The School will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in School classrooms or any changing facility.

4.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required the School will deactivate them.

5. The data protection principles

5.1. Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Objectives

6.1. The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

7. Protocols

7.1. The surveillance system will be registered with the ICO in line with data protection legislation.

7.2. The surveillance system is a closed digital system which does not record audio.

7.3. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

7.4. The surveillance system has been designed for maximum effectiveness and efficiency; however, the School cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

7.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

7.6. The surveillance system will not be trained on private vehicles or property outside the perimeter of the School.

8. Security

8.1. Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

8.2. The School's authorised CCTV system operators are:

- The Principal.
- The Operations Director.
- The DPO.
- The Compliance Manager.
- The Premises Manager.

8.3. The main control facility is kept secure and locked when not in use.

8.4. If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

8.5. Surveillance and CCTV systems will be tested for security flaws periodically to ensure that they are being properly maintained at all times.

8.6. Surveillance and CCTV systems will not be intrusive.

8.7. The Operations Director and Principal will decide when to record footage, e.g. a continuous loop outside the School grounds to deter intruders.

8.8. Any unnecessary footage captured will be securely deleted from the School system.

8.9. Each system will have a separate audio and visual system that can be run independently of one another. Audio CCTV will only be used in the case of deterring aggressive or inappropriate behaviour.

8.10. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

8.11. Visual display monitors are located in the reception and the Operations Director's office.

9. Privacy by design

9.1. The use of surveillance cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.

9.2. A DPIA will be carried out prior to the installation of any surveillance and CCTV system.

9.3. If the DPIA reveals any potential security risks or other data protection issues, the School will ensure they have provisions in place to overcome these issues.

9.4. Where the School identifies a high risk to an individual's interests, and it cannot be overcome, the School will consult the ICO before they use CCTV, and the School will act on the ICO's advice.

9.5. The School will ensure that the installation of the surveillance and CCTV systems will always justify its means.

9.6. If the use of a surveillance and CCTV system is too privacy intrusive, the School will seek alternative provision.

10. Code of practice

10.1. The School understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

10.2. The School notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails.

10.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

10.4. All surveillance footage will be kept for 30 days for security purposes; the Operations Director and the DPO are responsible for keeping the records secure and allowing access.

10.5. The School has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

10.6. The surveillance and CCTV system is owned by the School and images from the system are strictly controlled and monitored by authorised personnel only.

10.7. The School will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the School, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the School's website.

10.8. The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point, the DPO, through which people can access information and submit complaints.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the School.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and

work to meet and maintain those standards in accordance with the law.

- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.

10.9. Be accurate and well maintained to ensure information is up-to-date.

11. Access

11.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. All disks containing images belong to, and remain the property of, the School.

11.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. The School will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, the School may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7. Requests by persons outside the School for viewing or copying disks, or obtaining digital recordings, will be assessed by the Operations Director, who will consult the DPO, on a case-by-case basis with close regard to data protection legislation.

11.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one month of receipt.

11.11. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

11.12. Where a request is manifestly unfounded or excessive, the School holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

11.13. In the event that a large quantity of information is being processed about an individual, the School will ask the individual to specify the information the request is in relation to.

11.14. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

11.15. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation.

11.16. Requests for access or disclosure will be recorded and the Principal will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and review

12.1. This policy will be monitored and reviewed on an annual basis by the DPO and the Operations Director.

12.2. The DPO will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

12.3. The Operations Director will communicate changes to this policy to all members of staff.

West Kirby School and College

Single Central Record Policy

June 2021

Written by:	Luke Cowell	**Date:**	June 2021
Last reviewed on:	June 2021		

Contents:

Statement of intent

At West Kirby School & College, we are committed to promoting the safety and wellbeing of our staff, pupils and visitors. Ensuring the safety of our School community is of paramount importance and, as a result, this policy has been created to establish a more comprehensive safer recruitment procedure so that pupils feel safe at School. An SCR is required as part of this process as it provides Schools with a record of all pre-employment checks, ensuring staff are safe to work in the School.

To ensure the School is recruiting suitable individuals for a role, employment checks will be carried out by the School, in line with the School's Safer Recruitment Policy. The checks will include identity checks, right to work in the UK checks, varying levels of DBS checks (depending on the role), as well as extended European Economic Area (EEA) checks for staff who have lived or worked outside the UK.

This policy outlines the School's procedure for maintaining an up-to-date SCR in line with government statutory requirements and guidance.

1. **Legal framework**

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The Data Protection Act 2018
- The General Data Protection Regulation
- The Education Act 2002
- Education (Pupil Referral Units) (Application of Enactments) (England) Regulations 2007
- The Non-Maintained Special Schools (England) Regulations 2015

1.2. This policy has been created with due regard to the following DfE guidance:

- DfE (2018) 'Keeping children safe in education'

2. **Roles and responsibilities**

2.1. The Principal is responsible for:

- Ensuring all prospective members of staff and all employed members of staff have the required level of DBS checks.
- Deciding whether any prospective member of staff who holds a criminal conviction is suitable to work within the School.
- Ensuring the identity of all existing and prospective employees.

2.2. The Operations Director is responsible for:

- Maintaining an up-to-date SCR by updating it upon employment of any member of staff, as well as recording the identity and background checks made for other visiting staff to School.
- Ensuring any cover teachers, volunteers, contractors and/or any other visiting party to School hold the relevant level of security check, including a DBS check.
- Analysing whether any members of staff or returning volunteers, contractors or any other visiting party require an updated DBS check.
- Ensuring the School obtains legible copies of documentation used to prove workers' right to work in the UK, e.g. a copy of a passport.
- Ensuring that documentation evidencing workers' right to work in the UK is up-to-date, especially if visas have an expiry date on them.
- Ensuring that the data stored in the SCR is stored safely.
- Acting in accordance with this policy.

2.3. The School staff are responsible for:

- Providing accurate and up-to-date information required for the SCR so that they can continue their employment at School.
- Informing the Principal / Operations Director of any changes in personal data or additions that need to be made to the SCR.

2.4. Volunteers, contractors and other visiting parties are responsible for:

- Providing accurate and up-to-date information required for the SCR, so that they can continue their employment at School.
- Informing the Principal of any changes in personal data or additions that need to be made to the SCR.

3. Contents of an SCR

3.1. The SCR will detail checks for any member of staff who will likely come in to contact with a pupil. This includes the following:

- Full time teachers, supply teachers and trainees
- All other School staff, e.g. senior leaders
- All members of the governing board
- Any other individual likely to work in close proximity to the School's pupils

3.2. When employing agency staff from a third-party organisation, the School will obtain written notification that the organisation has carried out all of the relevant checks.

3.3. The Principal or Operations Director must ensure that the individual who presents themselves on their first day of employment is the subject of all pre-employment checks.

3.4. A copy of photographic identification will be obtained.

3.5. School records will include the following:

- An identity check
- A barred list check
- An enhanced DBS check
- A teacher prohibition check
- Right to work in the UK check
- [School employees only] Professional qualifications check
- [Workers who have lived or worked outside the UK only] European Economic Area (EEA) check
- [Senior leaders (SLT) and for Governor / Director positions only] A section 128 check

3.6. The SCR will also detail the following relevant checks:

- Childcare disqualification
- Safeguarding training dates
- Safer recruitment training dates

4. Storage

4.1. There will be only one copy of the SCR created on an online spreadsheet, which is password protected.

4.2. The School will not keep copies of DBS certificates, but staff have to be prepared to present them upon request.

4.3. The School will keep a legible copy of employees' evidence for their right to work in the UK, e.g. a copy of their passport, in the SCR.

4.4. All other documentation, such as photocopied proof of qualifications, will be safely stored in a personnel file.

4.5. All certificates will be stored in accordance with the School's Data Protection Policy.

5. Monitoring and review

5.1. The SCR will be updated after each instance of an individual attending School in an employment or voluntary capacity, or when any variation to the fields on the SCR is required.

5.2. Records kept on School leavers will be removed from the SCR six months after their departure.

5.3. The SCR will be reviewed annually by the Principal and Operations Director, ensuring all safety checks are present and up-to-date.

West Kirby School and College

Records Management Policy June 2021

Written by:	Luke Cowell	**Date:**	June 2021
Last reviewed on:	June 2021		

Contents:

Statement of intent

West Kirby School & College is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible to the appropriate individuals. In line with the requirements of the GDPR, the school also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended.

The school has created this policy to outline how records are stored, accessed, monitored, retained and disposed of to meet the school's statutory requirements.

This document complies with the requirements set out in the GDPR and Data Protection Act 2018.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect.

The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

- General Data Protection Regulation (GDPR)
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018

1.2. This policy also has due regard to the following guidance:

- Information Records Management Society (IRMS) (2019) 'Information Management Toolkit for Schools'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2018) 'Careers guidance and access for education and training providers'

1.3. This policy will be implemented in accordance with the following school policies and procedures:

- Data Protection Policy
- Data and E-Security Breach Prevention and Management Plan
- Disposal of Records Log
- Information Asset Register
- Archived Files Log

2. Responsibilities

2.1. The whole school has a responsibility for maintaining its records and record-keeping systems in line with statutory requirements.

2.2. The Principal and Operations Director hold the overall joint responsibility for this policy and for ensuring it is implemented correctly.

2.3. The DPO is responsible for the management of records at the school.

2.4. The DPO is responsible for promoting compliance with this policy and reviewing the policy on an annual basis, in conjunction with the Principal and Operations Director.

2.5. The DPO is responsible for ensuring that all records are stored securely, in accordance with the retention periods outlined in this policy, and are disposed of safely and correctly.

2.6. All staff members are responsible for ensuring that any records they are responsible for (including emails) are accurate, maintained securely and disposed of correctly, in line with the provisions of this policy.

3. Management of pupil records

3.1. Pupil records are specific documents that are used throughout a pupil's time in the education system – they are passed to each school that a pupil attends and includes all personal information relating to them, e.g. date of birth, home address, as well as their progress and achievements.

3.2. The following information is stored on the front of a pupil record, and will be easily accessible:

- Forename, surname, and date of birth
- Unique pupil number
- Note of the date when the file was opened

3.3. The following information is stored inside the front cover of a pupil record, and will be easily accessible:

- Any preferred names
- Emergency contact details and the name of the pupil's doctor
- Any allergies or other medical conditions that are important to be aware of
- Names of people with parental responsibility, including their home address(es) and telephone number(s)
- Any other agency involvement, e.g. speech and language therapist
- Reference to any other linked files

3.4. The following information is stored in a pupil record, and will be easily accessible:

- Admissions form
- Details of any SEND
- If the pupil has attended an early years setting, the record of transfer
- Data collection or data checking form
- Annual written reports to parents
- National curriculum and agreed syllabus record sheets
- Notes relating to major incidents and accidents involving the pupil

- Any information about an EHC plan and support offered in relation to the EHC plan
- Medical information relevant to the pupil's on-going education and behaviour
- Any notes indicating child protection disclosures and reports
- Any information relating to exclusions
- Any correspondence with parents or external agencies relating to major issues, e.g. mental health
- Notes indicating that records of complaints made by parents or the pupil
- Examination results – pupil copy
- SATs results

3.5. The following information is subject to shorter retention periods and, therefore, will be stored separately in a personal file for the pupil in the school office:

- Attendance registers and information
- Absence notes and correspondence
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Accident forms – forms about major accidents will be recorded on the pupil record
- Consent to administer medication and administration records
- Copies of pupil birth certificates, passports etc.
- Correspondence with parents about minor issues, e.g. behaviour
- Pupil work
- Previous data collection forms that have been superseded

3.6. Hard copies of disclosures and reports relating to child protection are stored in a sealed envelope, in a securely locked filing cabinet in the DSL's office – a note indicating this is marked on the pupil's file.

3.7. Hard copies of complaints made by parents or pupils are stored in a file in the PA to The Principal's office – a note indicating this is marked on the pupil's file.

3.8. Actual copies of accident and incident information are stored separately on the school's management information system and held in line with the retention periods outlined in this policy – a note indicating this is marked on the pupil's file. An additional copy may be placed in the pupil's file in the event of a major accident or incident.

3.9. The school will ensure that no pupil records are altered or amended before transferring them to the next school that the pupil will attend (unless requiring amendment to correct an inaccuracy before the transfer).

3.10. The only exception to the above is if any records placed on the pupil's file have a shorter retention period and may need to be removed. In such cases, the DPO will remove these records.

3.11. Electronic records relating to a pupil's record will also be transferred to the pupils' next school. Section 12 of this policy outlines how electronic records will be transferred.

3.12. The school will not keep any copies of information stored within a pupil's record, unless there is a legitimate need, legal requirement, or ongoing legal action at the time during which the pupil leaves the school. The responsibility for these records will then transfer to the next school that the pupil attends (if appropriate).

3.13. If any pupil attends the school until statutory school leaving age, the school will keep the pupil's records in line with the school's retention schedule (section 4 of this policy).

3.14. The school will, wherever possible, avoid sending a pupil record by post. Where a pupil record must be sent by post, it will be sent by registered post, with an accompanying list of the files included. The school it is sent to is required to sign a copy of the list to indicate that they have received the files and return this to the school.

4. Retention of pupil records and other pupil-related information

4.1. The table below outlines the school's retention periods for individual pupil records and the action that will be taken after the retention period, in line with any requirements.

4.2. Electronic copies of any information and files will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Personal identifiers, contacts and personal characteristics		
Images used for identification purposes	For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Securely disposed of

Images used in displays	Whilst the pupil is at school	Securely disposed of
Images used for marketing purposes	In line with the consent period	Securely disposed of
Biometric data	For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Securely disposed of
Postcodes, names and characteristics	Whilst the pupil is at school, plus five years	Securely disposed of
House number and road	For the duration of the event/activity, plus one month	Securely disposed of
Admissions		
Register of admissions	Every entry in the admissions register will be preserved for a period of three years after the date on which the entry was made	Information is reviewed and the register may be kept permanently
Admissions (where the admission is successful)	Date of admission, plus one year	Securely disposed of
Admissions appeals (where the appeal is unsuccessful)	Resolution of the case, plus one year	Securely disposed of
In-year secondary school admissions	Whilst the pupil remains at the school, plus one year	Securely disposed of
Proof of address (supplied as part of the admissions process)	Current academic year, plus one year	Securely disposed of
Supplementary information submitted, including religious and medical information etc. (where the admission was successful)	Information added to the pupil file	Securely disposed of
Supplementary information submitted, including religious and medical	Retained until the appeals process is complete	Securely disposed of

information etc. (where the admission was not successful)		
All records relating to the creation and implementation of the Admissions Policy	Life of the policy, plus three years and then review	Securely disposed of
Pupils' educational records		
Pupils' educational records	Whilst the pupil remains at the school	Transferred to the next destination – if this is an independent school, home-schooling or outside of the UK, the file will be kept by the school and retained for the statutory period
Pupils' educational records	25 years after the pupil's date of birth	Reviewed and securely disposed of if no longer needed
Public examination results	Added to the pupil's record and transferred to next school	All uncollected certificates returned to the examination board
Internal examination results	Added to the pupil's record and transferred to next school	Transferred to the next school
Behaviour records	Added to the pupil's record and transferred to the next school Copies are held whilst the pupil is at school, plus one year	Securely disposed of
Exclusion records	Added to the pupil's record and transferred to the next school Copies are held whilst the pupil is at school, plus one year	Securely disposed of

Child protection information held on a pupil's record	Stored in a sealed envelope for the same length of time as the pupil's record Records also subject to any instruction given by the Independent Inquiry into Child Sex Abuse (IICSA)	Securely disposed of – shredded
Child protection records held in a separate file	25 years after the pupil's date of birth Records also subject to any instruction given by the IICSA	Securely disposed of – shredded
Curriculum returns	Current academic year, plus three years	Securely disposed of
Schemes of work	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Timetable	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Class record books	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Mark books	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Record of homework set	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Pupils' work	Current academic year, plus one year	Review at the end of each year and allocate a further retention period or securely dispose of
Education, training or employment destinations data	Whilst the pupil is at the school, plus three years or from the end of KS4, whichever is earliest	Securely disposed of
Attendance		

Attendance registers	Every entry is retained for a period of three years after the date on which the entry was made	Securely disposed of
Correspondence relating to any absence (authorised or unauthorised)	Current academic year, plus two years	Securely disposed of
Medical information and administration		
Permission slips	For the duration of the period that medication is given, plus one month	Securely disposed of
Medical conditions – ongoing management	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school, plus one year	Securely disposed of
Medical incidents that have a behavioural or safeguarding influence	Added to the pupil's record and transferred to the next school Copies held whilst the pupil is at school, plus 25 years	Securely disposed of
SEND		
SEND files, reviews and EHC plans, including advice and information provided to parents regarding educational needs and accessibility strategy	The pupil's date of birth, plus 31 years	Securely disposed of
Curriculum management		
SATs results	25 years after the pupil's date of birth (as stated on the pupil's record)	Securely disposed of
Examination papers	Until the appeals/validation process has been completed	Securely disposed of

Published Admission Number (PAN) reports	Current academic year, plus six years	Securely disposed of
Valued added and contextual data	Current academic year, plus six years	Securely disposed of
Self-evaluation forms (internal moderation)	Current academic year, plus one year	Securely disposed of
Self-evaluation forms (external moderation)	Retained until superseded	Securely disposed of
Pupils' work	Returned to pupils at the end of the academic year, or retained for the current academic year, plus one year	Securely disposed of
Extra-curricular activities		
Field file – information taken on school trips	Until the conclusion of the trip, plus one month Where a minor incident occurs, field files are added to the core system as appropriate	Securely disposed of
Financial information relating to school trips	Whilst the pupil remains at school, plus one year	Securely disposed of
Parental consent forms for school trips where no major incident occurred	Until the conclusion of the trip	Securely disposed of – shredded
Parental consent forms for school trips where a major incident occurred	25 years after the pupil's date of birth on the pupil's record (permission slips of all pupils on the trip will also be held to show that the rules had been followed for all pupils)	Securely disposed of – shredded
Educational visitors in school – sharing of personal information	Until the conclusion of the visit, plus one month	Securely disposed of
Family liaison officers and home-school liaison assistants		
Day books	Current academic year, plus two years	Reviewed and securely destroyed if no longer required

Reports for outside agencies	Duration of the pupil's time at school	Securely disposed of
Referral forms	Whilst the referral is current	Securely disposed of
Contact data sheets	Current academic year	Reviewed and securely destroyed if no longer active
Contact database entries	Current academic year	Reviewed and securely destroyed if no longer required
Group registers	Current academic year, plus two years	Securely disposed of
Catering and free school meal management		
Meal administration	Whilst the pupil is at school, plus one year	Securely disposed of
Meal eligibility	Whilst the pupil is at school, plus five years	Securely disposed of

5. Retention of staff records

5.1. The table below outlines the school's retention period for staff records and the action that will be taken after the retention period, in line with any requirements.

5.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff members' personnel file	Termination of employment, plus six years, unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file will be retained until the IICSA enquiries are complete	Securely disposed of
Annual appraisal and assessment records	Current academic year, plus six years	Securely disposed of
Sickness absence monitoring (where sickness pay is not paid)	Current academic year, plus three years	Securely disposed of

Sickness absence monitoring (where sickness pay is paid)	Current academic year, plus six years	Securely disposed of
Staff training (where training leads to CPD)	Length of time required by the CPD professional body	Securely disposed of
Staff training (except where the training relates to dealing with pupils, e.g. first aid or health and safety)	Retained in the personnel file	Securely disposed of
Staff training (where the training relates to pupils, e.g. safeguarding or other pupil-related training)	Date of the training, plus 40 years	Securely disposed of
Recruitment		
Records relating to the appointment of a new Principal (unsuccessful attempts)	Date of appointment, plus six months.	Securely disposed of
Records relating to the appointment of a new Principal (successful appointments)	Added to personnel file and retained until the end of appointment, plus six years, except in cases of negligence or claims of child abuse, then records are retained for at least 15 years	Securely disposed of
Records relating to the appointment of new members of staff or governors (unsuccessful candidates)	Date of appointment of successful candidate, plus six months	Securely disposed of
Pre-employment vetting information (successful candidates)	For the duration of the employee's employment, plus six years	Securely disposed of
DBS certificates	Up to six months	Securely disposed of
Proof of identify as part of the enhanced DBS check	If it is necessary to keep a copy, it will be placed in the staff member's personnel file	Securely disposed of
Evidence of right to work in the UK	Added to staff personnel file or, if kept separately, termination of employment, plus no longer than two years	Securely disposed of

Annual leave records	For the duration of the employee's employment, plus six years	Securely disposed of
Change of personal details notifications	No longer than 6 months after receiving the request	Securely disposed of
Emergency contact details	Destroyed on termination	Securely disposed of
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards	Securely disposed of
Disciplinary and grievance procedures		
Child protection allegations, including where the allegation is unproven	Added to staff personnel file, and until the individual's normal retirement age, or 10 years from the date of the allegation – whichever is longer If allegations are malicious, they are removed from personal files If allegations are found, they are kept on the personnel file and a copy is provided to the person concerned unless the member of staff is part of any case which falls under the terms of reference of the IICSA. If this is the case, the file is retained until IICSA enquiries are complete	Reviewed and securely disposed of – shredded

Level 1 warning (oral)	Date of warning, plus six months (excluding the summer holiday)	Securely disposed of – if placed on staff personnel file, removed from file
Level 2 warning (written)	Date of warning, plus 9 months (excluding the summer holiday)	Securely disposed of – if placed on staff personnel file, removed from file
Level 3 warning (final written)	Date of warning, plus 12 months, which in exceptional cases may be for longer (excluding the summer holiday)	Securely disposed of – if placed on staff personnel file, removed from file
Records relating to unproven incidents	Conclusion of the case, unless the incident is child protection related, then it is disposed of as above	Securely disposed of

6. Retention of senior leadership and management records

6.1. The table below outlines the school's retention periods for senior leadership and management records, and the action that will be taken after the retention period, in line with any requirements.

6.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Governing board		
Agendas for governing board meetings	One copy alongside the original set of minutes – all others disposed of without retention	Local archives consulted before secure disposal
Original, signed copies of the minutes of governing board meetings	Permanent – all other copies disposed of without retention	Shredded if they contain any sensitive or personal information, but the local archives will be consulted first
Reports presented to the governing board that are referred to in the minutes	Permanent – all others disposed of without retention	Local archives consulted and then securely disposed of

Meeting papers relating to the annual parents' meeting	Date of meeting, plus a minimum of six years	Securely disposed of
Instruments of government, including articles of association	Permanent	Local archives consulted and then securely disposed of
Trusts and endowments managed by the governing board	Permanent	Local archives consulted and then securely disposed of
Action plans created and administered by the governing board	Until superseded or whilst relevant	Securely disposed of
Policy documents created and administered by the governing board	Until superseded or whilst relevant	Securely disposed of
Records relating to complaints dealt with by the governing board or Principal	Current academic year, plus six years If negligence is involved, records are retained for the current academic year, plus 15 years If child protection or safeguarding issues are involved, the records are retained for the current academic year, plus 40 years	Reviewed for further retention in case of contentious disputes, then securely disposed of
Annual reports required by the DfE	Date of report, plus 10 years	Securely disposed of
Proposals concerning changing the status of the school	Date proposal accepted or declined, plus three years	Securely disposed of
Records relating to the appointment of co-opted governors	Date of election, plus six months	Securely disposed of
Records relating to the election of the chair of the governing board and the vice chair	Destroyed after the decision has been recorded in the minutes	Securely disposed of
Scheme of delegation and terms of reference for committees	Until superseded or whilst relevant	Reviewed and offered to the local archives if appropriate

Meeting schedule	Current academic year	Standard disposal
Register of attendance at full governing board meetings	Date of last meeting in the book, plus six years	Securely disposed of
Records relating to governor monitoring visits	Date of the visit, plus three years	Securely disposed of
Correspondence sent and received by the governing board or Principal	Current academic year, plus three years	Securely disposed of
Records relating to the appointment of the clerk to the governing board	Date on which the clerk's appointment ends, plus six years	Securely disposed of
Records relating to the terms of office of serving governors, including evidence of appointment	Date on which the governor's appointment ends, plus six years	Securely disposed of
Records relating to governor declaration against disqualification criteria	Date on which the governor's appointment ends, plus six years	Securely disposed of
Register of business interests	Date the governor's appointment ends, plus six years	Securely disposed of
Governor code of conduct	Dynamic document – kept permanently	Securely disposed of
Records relating to the training required and received by governors	Date the governor steps down, plus six years	Securely disposed of
Records relating to the induction programme for new governors	Date on which the governor's appointment ends, plus six years	Securely disposed of
Records relating to DBS checks carried out on the clerk and members of the governing board	Date of the DBS check, plus six months	Securely disposed of
Governor personnel files	Date on which the governor's appointment ends, plus six years	Securely disposed of
Principal and SLT		
Log books of activity in the school maintained by the Principal	Date of last entry, plus a minimum of six years	Reviewed and offered to the local archives if appropriate
Minutes of SLT meetings and the meetings of other internal administrative bodies	Date of the meeting, plus three years	Reviewed annually and securely disposed of if not needed
Reports created by the Principal or SLT	Date of the report, plus a minimum of three years	Reviewed annually and securely disposed of if not needed

Records created by the Principal, Deputy Head Teacher, heads of year and other members of staff with administrative responsibilities	Current academic year, plus six years	Reviewed annually and securely disposed of if not needed
Correspondence created by the Principal, Deputy Head Teacher, heads of year and other members of staff with administrative responsibilities	Date of correspondence, plus three years	Securely disposed of
Professional development plan	Held on the individual's personnel record. If not, then it is retained for the duration of the plan, plus six years	Securely disposed of
SDP	Duration of the plan, plus three years	Securely disposed of

7. Retention of health and safety records

7.1. The table below outlines the school's retention periods for health and safety records, and the action that will be taken after the retention period, in line with any requirements.

7.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and safety		
Health and safety policy statements	Duration of policy, plus three years	Securely disposed of
Health and safety risk assessments	Duration of risk assessment, plus three years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Securely disposed of

Records relating to any reportable death, injury, disease or dangerous occurrence under RIDDOR	Date of incident, plus three years provided that all records relating to the incident are held on the personnel file	Securely disposed of
Accident reporting – adults	Three years after the last entry in the accident reporting book	Securely disposed of
Accident reporting – pupils	Three years after the last entry in the accident reporting book	Securely disposed of
Records kept under the Control of Substances Hazardous to Health Regulations	Date of incident, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation (maintenance records or controls, safety features and PPE)	Two years from the date on which the examination was made	Securely disposed of
Information relating to areas where employees and persons are likely to come into contact with radiation (dose assessment and recording)	Until the person to whom the record relates would have reached 75-years-old, but in any event for at least 30 years from when the record was made	Securely disposed of
Fire precautions log books	Current academic year, plus three years	Securely disposed of
Health and safety file to show current state of buildings, including all alterations (wiring, plumbing, building works etc.) to be passed on in the case of change of ownership	Permanent	Passed to new owner on sale or transfer of building

8. Retention of financial records

8.1. The table below outlines the school's retention periods for financial records and the action that will be taken after the retention period, in line with any requirements.

8.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll and pensions		
Maternity pay records	Current academic year, plus three years	Securely disposed of
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current academic year, plus six years	Securely disposed of
Timesheets, clock cards and flexitime records	Current academic year, plus three years	Securely disposed of
Absence record	Current academic year, plus three years	Securely disposed of
Batches	Current academic year, plus six years	Securely disposed of
Bonus sheets	Current academic year, plus three years	Securely disposed of
Car allowance claims	Current academic year, plus three years	Securely disposed of
Car loans	Current academic year, plus three years	Securely disposed of
Car mileage outputs	Current academic year, plus six years	Securely disposed of

Elements	Current academic year, plus two years	Securely disposed of
Income tax form P60	Current academic year, plus six years	Securely disposed of
Insurance	Current academic year, plus six years	Securely disposed of
Members allowance register	Current academic year, plus six years	Securely disposed of
National insurance – schedule of payments	Current academic year, plus six years	Securely disposed of
Overtime	Current academic year, plus three years	Securely disposed of
Part-time fee claims	Current academic year, plus six years	Securely disposed of
Pay packet receipt by employee	Current academic year, plus two years	Securely disposed of
Payroll awards	Current academic year, plus six years	Securely disposed of
Payroll (gross/net weekly or monthly)	Current academic year, plus six years	Securely disposed of

Payroll reports	Current academic year, plus six years	Securely disposed of
Payslips (copies)	Current academic year, plus six years	Securely disposed of
Pension payroll	Current academic year, plus six years	Securely disposed of
Personal bank details	Until superseded, plus three years	Securely disposed of
Sickness records	Current academic year, plus three years	Securely disposed of
Staff returns	Current academic year, plus three years	Securely disposed of
Superannuation adjustments	Current academic year, plus six years	Securely disposed of
Superannuation reports	Current academic year, plus six years	Securely disposed of
Tax forms	Current academic year, plus six years	Securely disposed of
Risk management and insurance		
Employer's liability insurance certificate	Closure of the school, plus 40 years	Securely disposed of Passed to the LA if the school closes
Asset management		

Inventories of furniture and equipment	Current academic year, plus six years	Securely disposed of
Burglary, theft and vandalism report forms	Current academic year, plus six years	Securely disposed of
Accounts and statements including budget management		
Annual accounts	Current academic year, plus six years	Disposed of against common standards
Loans and grants managed by the school	Date of last payment, plus 12 years	Information is reviewed then securely disposed of
All records relating to the creation and management of budgets	Duration of the budget, plus three years	Securely disposed of
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus six years	Securely disposed of
Records relating to the collection and banking of monies	Current financial year, plus six years	Securely disposed of
Records relating to the identification and collection of debt	Final payment, plus six years	Securely disposed of
Contract management		
All records relating to the management of contracts under seal	Last payment on the contract, plus 12 years	Securely disposed of
All records relating to the management of contracts under signature	Last payment on the contract, plus six years	Securely disposed of
All records relating to the monitoring of contracts	Life of the contract, plus six or 12 years	Securely disposed of
School fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus six years	Securely disposed of
School meals		
FSM registers (where the register is used as a basis for funding)	Current academic year, plus six years	Securely disposed of
School meals registers	Current academic year, plus three years	Securely disposed of

School meals summary sheets	Current academic year, plus three years	Securely disposed of
Pupil finance		
Student grant applications	Current academic year, plus three years	Securely disposed of
Pupil premium fund records	Date the pupil leaves the school, plus six years	Securely disposed of

9. Retention of other school records

9.1. The table below outlines the school's retention periods for any other records held by the school, and the action that will be taken after the retention period, in line with any requirements.

9.2. Electronic copies of any information and files will also be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property management		
Title deeds of properties belonging to the school	Permanent	Transferred to new owners if the building is leased or sold
Plans of property belonging to the school	For as long as the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus six years	Securely disposed of
Records relating to the letting of school premises	Current financial year, plus six years	Securely disposed of
Maintenance		
All records relating to the maintenance of the school carried out by contractors	For as long as the school owns the building and then passed onto any new owners if the building is leased or sold	Securely disposed of
All records relating to the maintenance of the school carried out by school employees	For as long as the school owns the building and then passed onto any new owners if the building is leased or sold	Securely disposed of

Operational administration		
General file series	Current academic year, plus five years	Reviewed and securely disposed of
Records relating to the creation and publication of the school brochure and/or prospectus	Current academic year, plus three years	If a copy is not preserved by the school, standard disposal
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current academic year, plus one year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year, plus one year	One copy archived, other copies standard disposal
Visitors' books and signing-in sheets	Last entry in the logbook, plus six years	Reviewed then securely disposed of
Records relating to the creation and management of parent-teacher associations and/or old pupil associations	Current academic year, plus six years	Reviewed then securely disposed of
Walking bus registers	Date of register, plus six years	Securely disposed of
School privacy notice which is sent to parents	Until superseded, plus six years	Standard disposal
Consents relating to school activities	While pupil attends the school	Secure disposal
CCTV Footage	30 days from date of footage	Securely disposed of

10. Retention of emails

10.1. Group email addresses will have an assigned member of staff who takes responsibility for managing the account and ensuring the correct disposal of all sent and received emails.

10.2. All staff members with an email account will be responsible for managing their inbox.

10.3. Staff will retain emails (that contain data that falls under the scope of the school's retention schedule) in line with the period of retention specified in the schedule (section 4-9 of this policy).

10.4. Personal emails, i.e. emails that do not relate to work matters or are from family members, will be deleted as soon as they are read.

10.5. Staff members will review and delete any emails they no longer require at the end of every term and that do not fall under the school's retention schedule, or that exceed the period of time for retention that is specified in the retention schedule.

10.6. Staff members will not, under any circumstances, create their own email archives, e.g. saving emails on to personal hard drives.

10.7. Staff members will be aware that the emails they send could be required to fulfil a SAR. Emails will be drafted carefully, and staff members will review the content before sending.

10.8. Staff members will discuss any queries regarding email retention with the DPO.

11. Identifying information

11.1. Under the GDPR, all individuals have the right to data minimisation and data protection by design and default – as the data controller, the school ensures appropriate measures are in place for individuals to exercise this right.

11.2. Wherever possible, the school uses pseudonymisation, uses initials, or uses redaction, also known as the 'blurring technique', to reduce the risk of identification.

11.3. Once an individual has left the school, if identifiers such as names and dates of birth are no longer required, these are removed or less specific personal data is used, e.g. the month of birth rather than specific date – the data is blurred slightly.

11.4. Where data is required to be retained over time, e.g. attendance data, the school removes any personal data not required and keeps only the data needed – in this example, the statistics of attendance rather than personal information.

12. Storing and protecting information

12.1. The DPO will undertake a business impact assessment to identify which records are vital to school management and these records will be stored in the most secure manner.

12.2. The IT Manager will conduct a back-up of information on a termly basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

12.3. Where possible, backed-up information will be stored off the school premises, using a central back-up cloud service operated by the school's IT provider. The IT Manager will ensure that the location of the cloud storage and the security offered is appropriate for the information and records stored on it.

12.4. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access.

12.5. Any room or area where personal or sensitive data is stored will be locked when unattended.

12.6. Confidential paper records are not left unattended or in clear view when held in a location with general access.

12.7. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed-up off-site.

12.8. **SLT ONLY:** Where data is saved on removable storage or a portable device, the device is kept in a locked and fireproof filing cabinet, drawer or safe when not in use.

12.9. Memory sticks are not permitted to be used to hold personal information.

12.10. All electronic devices are password-protected to protect the information on the device in case of theft.

12.11. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

12.12. Staff do not use their personal laptops or computers for school purposes.

12.13. All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

12.14. Emails containing sensitive or confidential information are password-protected or sent via a secure encrypted or data transfer system to ensure that only the recipient is able to access the information. The password will be shared with the recipient in a separate email.

12.15. Personal information is never put in the subject line of an email.

12.16. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

12.17. When sending confidential information by fax, members of staff always check that the recipient is correct before sending.

12.18. Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

12.19. If documents that have been taken off the school premises will be left unattended, the staff member will leave the documents in the locked boot of a car or keep them on their person.

12.20. A record will be kept of any document that is taken off the school premises that logs the location of the document and when it is returned to the school site, this includes records that are digitally remotely accessed.

12.21. Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

12.22. The school has data sharing agreements with all data processors and third parties with whom data is shared. These agreements are developed by the DPO and cover information about issues such as access controls and permissions.

12.23. A record is kept of what level of access each staff member has to data. This record details information including:

- What level of access each staff member has.
- Limits on how staff members access data.
- What actions staff members can perform.
- What level of access is changed or retained when a staff member changes role within the school.
- Who is able to authorise requests to change permissions and access.

12.24. All staff members implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information is stored in a securely locked filing cabinet, drawer or safe with restricted access.

12.25. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.

12.26. Staff are required to use their school login details to use photocopiers and printers.

12.27. The physical security of the school's buildings, and access to them, is reviewed termly by the Premises Manager in conjunction with the Operations Director. If an increased

risk in vandalism, burglary or theft is identified, this will be reported to the Principal and extra measures to secure data storage will be put in place.

12.28. All systems that allow staff and pupils to remotely access information from the school's network whilst they are not physically at the school have strong security controls in place which are reviewed termly by the DPO and IT Manager.

12.29. The DPO decides what restrictions are necessary to prevent information or records being downloaded, transferred or printed while the user is not on the school site.

12.30. The school takes its duties under the GDPR seriously and any unauthorised disclosures may result in disciplinary action.

12.31. The DPO is responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

12.32. Any damage to or theft of data will be managed in accordance with the school's Data and E-Security Breach Prevention and Management Policy & Plan.

13. Accessing information

13.1. We are transparent with data subjects, the information we hold and how it can be accessed.

13.2. All members of staff, parents of registered pupils and other users of the school, e.g. visitors and third-party clubs, are entitled to:

- Know what information the school holds and processes about them or their child and why.
- Understand how to gain access to it.
- Understand how to provide and withdraw consent to information being held.
- Understand what the school is doing to comply with its obligations under the GDPR.

13.3. All members of staff, parents of registered pupils and other users of the school and its facilities have the right, under the GDPR, to access certain personal data being held about them or their child.

13.4. Personal information can be shared with pupils once they are considered to be at an appropriate age and responsible for their own affairs; although, this information can still be shared with parents.

13.5. Pupils who are considered by the school to be at an appropriate age to make decisions for themselves are entitled to have their personal information handled in accordance with their rights.

13.6. The school will adhere to the provisions outlined in the school's Data Protection Policy when responding to requests seeking access to personal information.

14. Digital continuity statement

14.1. Digital data that is retained for longer than six years will be identified by the DPO and named as part of a digital continuity statement.

14.2. The data will be archived to dedicated files on the school's server, which are password-protected – this will be backed-up in accordance with section 12 of this policy.

14.3. Memory sticks are never used to store digital data, subject to a digital continuity statement.

14.4. The IT Manager will review new and existing storage methods annually and, where appropriate add them to the digital continuity statement.

14.5. The following information will be included within the digital continuity statement:

- A statement of the business purposes and statutory requirements for keeping the records
- The names of the individuals responsible for long term data preservation
- A description of the information assets to be covered by the digital preservation statement
- A description of when the record needs to be captured into the approved file formats
- A description of the appropriate supported file formats for long-term preservation
- A description of the retention of all software specification information and licence information
- A description of how access to the information asset register is to be managed in accordance with the GDPR

15. Information audit

15.1. The school conducts information audits on an annual basis against all information held by the school to evaluate the information the school is holding, receiving and using,

and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Microfilm or microfiche
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Knowledge
- Apps and portals

15.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

15.3. The DPO is responsible for completing the information audit (either in person or through a 3rd party). The information audit will include the following:

- The school's data needs
- The information needed to meet those needs
- The format in which data is stored
- How long data needs to be kept for
- Vital records status and any protective marking
- Who is responsible for maintaining the original document

15.4. The DPO will consult with staff members involved in the information audit process to ensure that the information is accurate.

15.5. Once it has been confirmed that the information is accurate, the DPO will record all details on the school's Data Asset Register.

15.6. An information asset owner is assigned to each asset or group of assets. They will be responsible for managing the asset appropriately, ensuring it meets the school's requirements, and for monitoring risks and opportunities.

15.7. The information displayed on the Data Asset Register will be shared with the Principal and Operations Director to gain their approval.

16. Disposal of data

16.1. Where disposal of information is outlined as standard disposal, this will be recycled appropriate to the form of the information, e.g. paper recycling, electronic recycling.

16.2. Where disposal of information is outlined as secure disposal, this will be shredded, pulped or destroyed by a confidential waste paper merchant, and electronic information will be scrubbed clean and, where possible, cut, archived or digitalised. The DPO will keep a record of all files that have been destroyed.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member will record in this list at least: -

- File reference (or other unique identifier);
- File title/description;
- Number of files;
- Name of the authorising Officer;
- Date destroyed or deleted from system; and
- Person(s) who undertook destruction.

16.3. Where the disposal action is indicated as reviewed before it is disposed, the DPO will review the information against its administrative value – if the information should be kept for administrative value, the DPO will keep a record of this.

16.4. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

16.5. Where information has been kept for administrative purposes, the DPO will review the information again after three years and conduct the same process. If it needs to be destroyed, it will be destroyed in accordance with the disposal action outlined in this policy. If any information is kept, the information will be reviewed every three subsequent years.

16.6. Where information must be kept permanently, this information is exempt from the normal review procedures.

16.7. Records and information that might be of relevant to the Independent Inquiry into Child Sexual Abuse (IICSA) will not be disposed of or destroyed.

17. School closures and record keeping

Academy conversion

17.1. If the school closes and subsequently becomes an academy, all records relating to pupils who are transferring to the academy will be transferred.

17.2. If the school will retain the existing building when it converts to an academy, all records relating to the management of the buildings will be transferred.

Sale or re-use of the site

17.3. If the school site is being sold or re-allocated to another use, the relevant LAs will take responsibility for the records of pupils from each specific LA from the date the school closes.

Merger of schools

17.4. If the school merges with another school to create one school, the new school will be responsible for retaining all current records originating from the former schools.

17.5. The DPO will determine the outcome of each group of records; these outcomes are as follows:

- Securely destroy all records that are expired and due for disposal, in accordance with the retention periods outlined in this policy.
- Transfer to the successor school or academy all records that are current and that will be required by the new school or academy.
- Transfer to each LA all records that are dormant but still need to be retained to comply with legal and business retention requirements.
- Transfer to the local record office any records with historical value.

Managing records

17.6. The DPO will identify which records need to be destroyed or transferred to the relevant body – they will allocate personnel as necessary to sort through records.

17.7. The DPO will notify the other organisations as soon as possible so that necessary disposal, storage and transfer arrangements can be made. The school's IT provider will also be notified so that arrangements can be made to ensure the safe transfer or deletion of electronic records, including all back-up copies.

17.8. When sorting records, the DPO and their team will:

- Review all records held within the school as soon as notification of closure is received, including paper and electronic records.
- Use the retention periods outlined in this policy to categorise the records into those to be destroyed and those that need to be transferred

- Contact the relevant body to make arrangements for the safe and secure transfer of records.
- Sort, list and box the records in preparation for the transfer, ensuring records are stored in a safe environment whilst awaiting collection.
- Plan how the disposal of records will be undertaken.
- Sort expired records in readiness for confidential disposal, ensuring they are stored securely whilst awaiting disposal.

17.9. All forms of storage will be completely emptied before the building is vacated or before disposal.

17.10. Records awaiting transfer will be held in a secure area.

17.11. The identity of any third parties collecting or disposing of records will be checked and a collection receipt will be obtained.

17.12. Records will be disposed of in line with section 16 of this policy.

17.13. Electronic records will be either transferred to the new body or deleted.

17.14. All IT equipment will be decommissioned in accordance with the school's processes.

17.15. No records will be left behind once the school building is vacated.

18. Monitoring and review

18.1. This policy will be reviewed on an annual basis by the DPO in conjunction with the Operations Director and Principal.

18.2. Any changes made to this policy will be communicated to all members of staff and the governing board.

Privacy Notice for Governors / Trustees and other Volunteers

Under data protection law, individuals have a right to be informed about how the School / Charity uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals working with the School / Charity in a voluntary capacity, including governors/trustees.

We, West Kirby School & College ('WKRS' / 'WKS' / 'West Kirby Residential School') are the 'data controllers' for the purposes of data protection law.

Our data protection officer is Pete Smith. He can be contacted at psmith@wkrs.co.uk.

The personal data we hold

We process data relating to those volunteering at our School / Charity. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- References
- Evidence of qualifications
- Employment details
- Information about business and pecuniary interests

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This may include information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Disability and access requirements

Why we use this data

The purpose of processing this data is to help us run the School / Charity to:

- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing Governors' / Trustees' details
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Undertake equalities monitoring

- Ensure that appropriate access arrangements can be provided for volunteers who require them

Our legal basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify our use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

Personal data is stored in line with our data protection policy.

We maintain a file to store personal information about all Governors / Trustees and other Volunteers.

The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the School / Charity.

When your relationship with the School / Charity has ended, we will retain and dispose of your personal information in accordance with our data protection policy.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Government departments or agencies – to meet our legal obligations to share information about Governors / Trustees
- Our local authority – to meet our legal obligations to share certain information with it, such as details of Governors
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as Governor / Trustee support
- Professional advisers and consultants
- Employment and recruitment agencies
- Police forces, courts

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Use of your personal information for marketing purposes

Where you have given us consent to do so, the School / Charity may send you marketing information by e-mail or text promoting School / Charity events, campaigns, charitable causes or services that may be of interest to you. You can "opt out" of receiving these texts and/or e-mails at any time by clicking on the "Unsubscribe" link at the bottom of any such communication, or by contacting our data protection officer.

Your rights

How to access personal information we hold about you

Individuals have a right to make a 'subject access request' to gain access to personal information that the School / Charity holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have a right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Pete Smith – psmith@wkrs.co.uk

Privacy Notice for Prospective Employees

Businesses are currently required to detail to staff how their personal data may be collected and used.

Who processes your information?

The School / Charity is the data controller of the personal information you provide to us. This means they determine the purposes for which, and the manner in which, any personal data relating to prospective employees is to be processed.

Pete Smith is the Data Protection Officer (DPO). Their role is to oversee and monitor the School's / Charity's data processing practices. This individual can be contacted on 0151 632 3201 or psmith@wkrs.co.uk.

Where necessary, third parties may be responsible for processing prospective employees' personal Information (i.e. external recruitment agencies). Where this is required, the School / Charity places data protection requirements on third party processors to ensure data is processed in line with staff members' privacy rights.

Why do we need your information?

The Charity / School, West Kirby School & College ('WKS', 'WKRS', 'West Kirby Residential School'), has the legal right and a legitimate interest to collect and process personal data relating to those whio apply to be employed and work at the School / Charity.

We process personal data in order to meet the safeguarding requirements set out in UK employment and childcare law, including those in relation to the following:

- Safeguarding Vulnerable Groups Act 2006
- Keeping Children Safe in Education 2016
- The Childcare (Disqualification) Regulations 2009

Prospective employees' personal data is also processed to enable the selection of suitably experienced and qualified staff to work at (and be employed by) the School / Charity.

What categories of data are processed?

The categories of personal information that we process include the following:

- Personal information – e.g. name, contact details, National Insurance number
- Characteristics information – e.g. gender, age, ethnic group
- Qualifications and, where relevant, the subjects taught
- Recruitment information – e.g. documentation relating to employment checks, references

This list is not exhaustive – to access the current list of information the Charity / School processes, please contact our HR Team.

Which data is collected?

The personal data we will collect from prospective employees of the School / Charity includes the following:

- Your name, address and contact details, including email address and telephone number;
- Details of your qualifications, skills, experience and employment history;
- Information about your current level of remuneration, including benefit entitlements;
- Whether or not you have a disability for which the University needs to make reasonable adjustments during the recruitment process;
- Information about your eligibility to work in the UK; and
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, disability and religion or belief.

The School / Charity may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

The School / Charity may also collect personal data about you from third parties, such as health questionnaire information from our Occupational Health service to help ensure the School / Charity considers additional control measures where and when required, information from criminal records checks etc.

The School / Charity may seek information from third parties prior to, or after, a job offer that has been made to you and will inform you that it is doing so. This may involve contacting your referees before a job offer is made.

Data will be stored in a range of different places, including on your application record, in HR and Payroll systems and on other IT systems (including email).

Why does the School / Charity process personal data?

The School / Charity needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, the School / Charity needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The School / Charity has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the School / Charity to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The School / Charity may also need to process data from job applicants to respond to and defend against legal claims.

The School / Charity may process information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where the School / Charity processes other special categories of data, such as information about ethnic origin, sexual orientation, disability or religion or belief, this is for equal opportunities monitoring purposes.

For some roles, the School / Charity is obliged to seek information about criminal convictions and offences.

Where the School / Charity seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The School / Charity will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to your data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, shortlisting and interview panel members involved in the recruitment process (this may include external panel members), other managers in the Department / Charity / School with a vacancy (where appropriate) and IT staff if access to the data is necessary for the performance of their roles.

The School / Charity may share your data with third parties, prior to any application for employment that is successful and it makes you an offer of employment.

As well as circulating your application and related materials to the appropriate staff at the School / Charity, we will share your personal information for the above purposes as relevant and necessary with:

- Your referees.
- Disclosure & Barring Service (DBS) in order to administer relevant recruitment checks and procedures.
- UK Visas & Immigration (UKVI) in order to administer relevant recruitment checks and procedures.
- Where relevant and as required for some posts, NHS organisations or similar organisations (e.g. NHS Trusts or Local Education Training Boards).
- Companies or organisations providing specific services to, or on behalf of, the University (e.g. RUH Occupational Health Service).

Your data may be transferred outside the European Economic Area (EEA) in order to meet our contractual obligations with you (e.g. to conduct reference checks). Such transfers are carried out with appropriate safeguards in place to ensure the confidentiality and security of your personal information.

How does the School / Charity protect your personal data?

The School / Charity takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. Further details about the School's / Charity's security procedures in relation to HR-related data can be found in our data protection policies.

How long is your data retained for?

If your application for employment is unsuccessful, the School / Charity will hold all your data electronically, and on the hard-copy recruitment file for 6 months after the end of the relevant recruitment process (except if the person appointed to the post is sponsored under the UK's points-based immigration system, when the School / Charity is required to retain the applications of all candidates shortlisted for final interview for 6 months or until UK Visas & Immigration (UKVI) have examined and approved them, whichever is the longer period). All non-personal data will be deleted and permanently destroyed after this point.

If your application for employment is successful, the School / Charity will hold all your personal data gathered during the recruitment process, which will be transferred to your personnel file (in hard copy or electronic format, or both), and on HR and Payroll systems and retained for the duration of your employment. The periods for which your data will be held on our HR and Payroll systems are set-out in the School's / Charity's Data Retention Policy.

Wherever possible we will not retain original documents or print-outs and instead will make a note on our central HR and Payroll system that the relevant check or procedure has been completed.

What are your rights?

As the data subject, you have specific rights to the processing of your data.

You have a legal right to:

- Access and obtain a copy of your data on request;
- Require the School / Charity to change incorrect or incomplete data;
- Require the School / Charity to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- Object to the processing of your data where the School / Charity is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact the School's / Charity's Data Protection Officer using the contact details provided at the end of this Privacy Notice. If you believe that the School / Charity has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to the School / Charity during the recruitment process. However, if you do not provide the information, the School / Charity may not be able to process your application properly or at all.

Automated decision making

Recruitment processes are not based solely on automated decision-making.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Pete Smith – psmith@wkrs.co.uk

Privacy Notice for Staff / Employees

Businesses are currently required to detail to staff how their personal data may be collected and used.

Who processes your information?

The School / Charity is the data controller of the personal information you provide to us. This means they determine the purposes for which, and the manner in which, any personal data relating to staff is
to be processed.

Pete Smith is the Data Protection Officer (DPO). Their role is to oversee and monitor the School's / Charity's data processing practices. This individual can be contacted on 0151 632 3201 or psmith@wkrs.co.uk.

Where necessary, third parties may be responsible for processing staff members' personal information. Where this is required, the School / Charity places data protection requirements on third
party processors to ensure data is processed in line with staff members' privacy rights.

Why do we need your information?

The Charity / School, West Kirby School & College ('WKS', 'WKRS', 'West Kirby Residential School'), has the legal right and a legitimate interest to collect and process personal data relating to those we employ to work at the School / Charity, or those otherwise contracted to work at the School / Charity.

We process personal data in order to meet the safeguarding requirements set out in UK employment and childcare law, including those in relation to the following:

- Safeguarding Vulnerable Groups Act 2006
- Keeping Children Safe in Education 2019
- The Childcare (Disqualification) Regulations 2009

Staff members' personal data is also processed to assist in the running of the School / Charity, and to enable individuals to be paid.

If staff members fail to provide their personal data, there may be significant consequences. This

includes the following:

Employment checks:

- Failure to provide the charity with ample proof of a right to work in the UK will prevent employment at the School / Charity.
- Failure to supply all safer recruitment documents and evidence will prevent employment at the School / Charity.
- Employees found to be working illegally could face prosecution by law enforcement officers.

Medical Information:

- Failure to provide the School / Charity with medical information which will impact your ability to perform your role will not enable the School / Charity to offer support and make reasonable adjustments.

Salary requirements:

- Failure to provide accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or an employee paying too much tax.

For which purposes are your personal data processed?

In accordance with the above, staff members' personal data is used for the following reasons:

- Contractual requirements
- Employment checks, e.g. right to work in the UK
- Salary requirements

Which data is collected?

The personal data the charity will collect from the School / Charity workforce includes the following:

- Names
- National insurance numbers
- Characteristics such as ethnic group
- Employment contracts
- Remuneration details
- Qualifications
- Absence information

Recruitment Information

The collection of personal information will benefit the School / Charity by:

- Improving the management of workforce data across the School / Charity.

- Ensuring the workforce is utilised to meet the pupil's needs.
- Enabling the development of a comprehensive picture of the workforce and how it is deployed.
- Informing the development of recruitment policies.
- Allowing better financial modelling and planning.
- Enabling ethnicity and disability monitoring.

Will your personal data be sought from third parties?

Staff members' personal data is only sought from the data subject. No third parties will be contacted to obtain staff members' personal data without the data subject's consent.

Staff members' personal data may be obtained and processed from third parties where the law requires the School / Charity to do so, e.g. medical records from a GP.

The categories of data obtained and processed from third parties include:

- Payroll- Pension Companies
- Medical – GP, Consultant, Occupational Health
- Medicash, Beneden
- Childcare Voucher Scheme
- Safeguarding – DBS, Disclosure by Association, Teachers
- Barring Services
- Department of Education
- Insurance Company
- Charity Solicitor

How is your information shared?

The charity will not share your personal information with any third parties without your consent, unless the law allows us to do so.

How long is your data retained for?

Staff members' personal data is retained in line with the School's / Charity's data retention policy.

Personal information may be retained for the following periods depending on the nature of the information.

Data will only be retained for as long as is necessary to fulfil the purposes for which it was processed, and will not be retained indefinitely.

If you require further information regarding retention of data, and the periods for which your personal data is held for, please refer to the School's / Charity's data retention policy.

How we store this data

Personal data is stored in line with our data protection policy.

We maintain a file to store personal information about all Staff and Employees.

The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the School / Charity.

When your relationship with the School / Charity has ended, we will retain and dispose of your personal information in accordance with our data protection policy and data retention policy.

What are your rights?

As the data subject, you have specific rights to the processing of your data.
You have a legal right to:

- Request access to the personal data that the charity holds.
- Request that your personal data is amended.
- Request that your personal data is erased.
- Request that the processing of your data is restricted.

Where the processing of your data is based on your explicit consent, you have the right to withdraw this consent at any time. This will not affect any personal data that has been processed prior to withdrawing consent.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Pete Smith – psmith@wkrs.co.uk