West Kirby School and College

E-safety Policy

Date Written: September 2020
Author: P Smith

Scope

This policy applies to all members of WKS (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both on and off school premises. The Education and Inspections Act 2006 empowers the Governors and Directors, as Accountable Body to delegate to the Principal to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is also pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers exercised by the Governors and Directors via its Principal with regard to the searching for and of electronic devices and the deletion of data.

WKS expects all staff and volunteers to address incidents of breaches of standards and practices with regard to e-safety through local management and professional action with pupils and adults having regard to associated behaviour management processes and procedures and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

This policy should be read alongside the Safeguarding Policy and Child Protection Procedures September 2020 and 'Keeping children safe in education' –statutory guidance for schools and colleges September 2020 (paying particular reference to Annex C: Online safety).

Policy Statement

WKS expects internet access and capability to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. WKS aims to equip the pupils with all the necessary ICT skills for modern life.

Some of the benefits of using ICT and the internet in schools are:

Pupils

- Access to worldwide educational resources and institutions to support all aspects of the curriculum and associated learning activities
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen
- Access to learning whenever and wherever convenient
- Freedom to be creative
- Freedom to explore the world and its cultures from within a classroom or similar learning setting
- Access to case studies, videos and interactive media to enhance understanding
- Individualised access to learning appropriate to age

Employees

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and learning settings strategies
- Immediate professional and personal support through networks and associations
- Improved access to technical support
- Ability to provide timely feedback to pupils and parents
- Class/learning activity management, attendance records, schedule, and assignment tracking

Authorising Internet Access

- All employees are required to read and sign the 'Acceptable Use Policy Agreement - Staff (and Volunteer)' before using any school ICT resource
- All pupils are asked to sign an Authorised Use Policy Sheet after discussing possible dangers of internet usage and preventative measures with staff.
- All pupils and employees are required to have a regulated set of passwords with unique identifiers and recorded as assigned to individuals.
- Pupils access to the internet will be in supervised activities with access to approved on-line materials
  (via Wirral Filter and Hi-impact)

Assessing Risks

WKS is expected to take all reasonable precautions to prevent access to inappropriate material. WKS is expected to have a procedure and system in place to monitor ICT use to establish if the e-safety procedure is adequate and that the implementation of the e-safety policy and related procedures are appropriate and effective.

Roles & Responsibilities

WKS's Governing Body is responsible for the approval of the school's procedures related to this E-Safety Policy and for reviewing the effectiveness of those procedures. This will be carried out by the Governors receiving regular information about e-safety and the Safeguarding Governor receiving additional information about incidents and monitoring reports

The Governing Body is expected to have within its lead governor portfolio a degree of awareness and oversight of the adequacy of school's systems to ensure e-safety. Lead Governor is the lead governor for Safeguarding and Child Protection. The governor oversight role includes:

- regular meetings with the school's E-Safety Co-ordinator
- validation that the school has regular monitoring of e-safety incident logs in place
- validation that the school has in place regular monitoring of filtering / change control logs

WKS is required to clearly identify the roles and responsibilities in relation to e-safety:

- Principal and Senior Managers

- The E-Safety Coordinators (Mr G Macdonald, G Hayes) with specific roles and responsibilities for e-safety procedures
- Teaching and Support Staff – especially staff involved in supervising residential provision
- Designated Safeguarding Lead/Deputy Designated Safeguarding Lead
- Pupils/Students
- Parents/Carers

WKS IT specialist Teacher (Mr G Macdonald) is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection procedure in which passwords are changed when needed
- the filtering procedures are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access /email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal/ Designated Safeguarding Lead/ ICT Steering Group/E-Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school procedures

Teaching and Learning

Teaching Staff are to clearly outline the use of ICT within the school's curriculum and the benefits to teaching & learning. The school procedures are expected to identify the control measures in place to reduce risk involved in the use of ICT within the curriculum as well as sanctions in the event of an incident. Both pupils and their parents/carers are required to sign a Home School Agreement (or similar arrangement) to ensure they have read, understood and agreed to the E-Safety rules as outlined in the school's E-safety procedures.

Web Filtering

Filtering strategies are selected in discussion with WKS's SLT & DSLs, Wirral (IP) and Hi Impact. The filtering strategy is selected to suit the age and curriculum requirements of the pupil.
Any material found that is believed to be unlawful will be reported to the appropriate regulatory agencies.

Managing Information Systems

The IT Manager is charged with establishing and maintaining effective web filtering technology and systems to support each school to maintain effective e-safety infrastructure.

The security of each school's information systems and users will be reviewed regularly by the IT Manager and virus protection software will be updated regularly.

WKS requires the following systems to be in place and adhered to:

- ensuring that all personal data sent over the internet is encrypted
- making sure that unapproved software is not downloaded to any school computers
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced
- Only designated pupils have access to upload any software to school system through external hard drives (these pupils will have earned Independent Status and be approved by staff)

Emails

All staff and pupils are expected to comply with WKS's Data Security, Protection & Retention Policy and to inform staff and pupils that school email accounts are only to be used for WKS / school-related matters, i.e. for staff to contact parents, pupils, other members of staff and other professionals for work purposes. The school has the right to monitor emails and their contents (Acceptable Use of Internet and Email by Staff).

Published Content and Websites

All websites operated in the name of the WKS/WKRS including school specific pages and presentations are required to comply with the highest standards of content maintenance.
Any information published on the website is to be carefully considered in terms of safety for the pupils, staff, copyrights and privacy policies. Limited information on staff or pupils is to be published and the only contact details for contacting the school will be via the school office or authorised staff school email addresses.
The Principal and IT Specialist teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Cross reference is required with the Charity's Data Security, Protection & Retention Policy especially relating to web posting of pupil images.

Social Networking and Social Media

Online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. A main aim of WKS is to educate pupils so that they can make their own informed decisions and take responsibility for their conduct online and have clear procedures in place with respect to social media.

The school's procedures are required to clearly state that pupils are not allowed to access social media sites in school unless explicitly for the purpose of school business and/or lessons (i.e. school twitter feed, etc.) Employees should restrict use of social media when in school to not include personal accounts. Personal use of social media should refrain from reference to employment activity and school life. Employment related potential use should be approved by the Principal of the school or a direct senior line manager. This social media activity should be monitored before publication (in

reference to school twitter comments) Further information is available in: Protocol for Acceptable use of Internet & Email by Staff.

Mobile phones and personal data devices

While mobile phones and personal communication devices are commonplace in today's society, WKS is expected to be aware of their use and ensure that mobile phones are used responsibly and at allotted times only. Only school equipment should be used to create digital images and/or video of school events, and/or the school population. Visitors are asked to turn off phones on entry into the school for the duration of their visit.

Handling E-safety Incidents

WKS procedures include clear instructions for all E-safety incidents including the roles and responsibilities to record the incident on our online 'Behaviour Watch' system, agree an action then monitor and review the incident. Depending on the severity of the incident, other parties may need to be involved at the discretion of the Principal and the school's Designated Safeguarding Lead/Deputy Designated Safeguarding Lead (referring to Safeguarding Children and Child Protection Policy 2020).

Cyberbullying

The anonymity that can come with using the internet increases the confidence in individuals to say and do hurtful things that they otherwise would not do in person.

Information about specific strategies or programmes in place to prevent and tackle bullying is to be set out in the Safeguarding, Behaviour and Anti-Bullying policies. It is to be made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in an investigation by senior staff and/or Designated Safeguarding Lead. WKS has a statutory duty to look after the physical and mental health of its employees. This includes protecting staff from cyberbullying and supporting the individual in the event of an incident. WKS is expected to:

- make staff aware of the potential risks of being bullied online through social networking sites by parents/carers and pupils
- train staff on how to protect themselves from cyberbullying
- ensure staff are aware on how to report incidents of cyberbullying and provide advice and support to the individual throughout the process

Further information can be found from the DfE guidance 'Cyberbullying: advice for Head teachers and school staff Nov 2014'.

Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. WKS is required to risk-assess any new technologies before they are used and ensure the technology provides educational

benefits. WKS is expected to keep up-to-date with new technologies and to be prepared to quickly develop appropriate strategies for dealing with new technological developments.

Monitoring

WKS will monitor any concerns relating to e-safety by:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity.

Additionally, WKS has a Safeguarding governor (Mr J Wylie) with a portfolio which includes e-safety to be kept updated in relation to issues and management action to ensure e-safety maintenance.

Parent Advice

Parents/carers play a vital role in the safety of children and young people online and each school is expected to provide guidance on e-safety through the following:

- Home School Agreement - ensure parents/carers understand the school's e-safety rules and procedures
- School website – provide links to validated third party advice on e-safety and publish DfE guidance such as 'Advice for parents and carers on cyberbullying '.
- Newsletters and emails

Acceptable Use Policy Agreement - Pupil

When I am using the computer or other technologies, I understand the need to feel safe all the time. I agree that I will:

- Always keep my passwords a secret
- Only visit sites which are appropriate to my work at the time
- Work in collaboration only with friends and I will deny access to others
- Tell a responsible adult straight away if anything makes me feel scared or uncomfortable
- Make sure all messages I send are respectful
- Show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- Not reply to any nasty message or anything which makes me feel uncomfortable
- Only e mail people I know or those approved by a responsible adult
- Only use e mail which has been provided by school
- Always keep my personal details private. (My name, family information, journey to school, my pets and hobbies, etc.)
- Always check with a responsible adult and my parents before I show photographs of myself
- Never meet an online friend without taking a responsible adult that I know with me

I know that once I post a message or an item on the internet then it is completely out of my control. I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

I agree that I will not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Inappropriate material
- Promoting discrimination of any kind
- Promoting illegal acts
- Break any school e-safety rule
- Do anything which exposes me or other children to danger

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be enforced.

Name:		**Year group:**
Signed:		**Date:**

Acceptable Use Policy Agreement - Staff (and Volunteer)

This Acceptable Use Policy is intended to ensure:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- Staff are protected from potential risk in their use of ICT in their everyday work

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website/ VLE) it will not be possible to identify by name, or other personal information, those who are featured
- I will only communicate with pupils and parents using official school systems and any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate material which may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings, unless permission is granted by the Principal
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted

  I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name:	Signed:	Date:

Parent/Carer Acceptable Use Policy Agreement Permission Form

Parent/Carers Name

Pupil Name

This Acceptable Use Policy is intended to ensure:

- Young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour

The school will try to ensure that students/pupils will have good access to ICT to enhance their learning and will, in return, expect the students/pupils to agree to be responsible users. A copy of the Student/ Pupil Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

As the parent/carer of the above pupils, I give permission for my son/daughter to have access to the internet and to ICT systems at school.
I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.
I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.
I understand that my son/daughter could access material outside of school and I will take every reasonable precaution, including monitoring and filtering to ensure my child will be safe whilst using the internet.

Signed

Date

Use of Digital / Video Images Permission Form

Parent / Carers Name

Pupil Name

The use of digital video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,
The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children.

Signed Date

As the parent/carer of the above pupil I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines and the school's Camera and Video Courtesy Code' in my use of these images.

Signed Date