



E-Safety and Acceptable Use Policy

Policy reviewed: September 2023

Approved by Governors:

To be read in conjunction with:

- Anti-bullying
- Equalities
- SEND
- Safeguarding
- Whistle Blowing
- Complaints
- Data protection and Freedom of Information



INNSWORTH SCHOOLS' PARTNERSHIP E-SAFETY AND ACCEPTABLE USE POLICY

Rationale

The purposes of Internet use in school include; to contribute to raising educational standards, to promote pupil achievement, to support the professional work of staff, to enhance the school's management functions and to enable remote learning when needed. The Internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children with quality Internet access as part of their learning experience. Children use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The school has responsibility for online safety inline with the requirements in KCSIE 2021. The Designated Safeguarding Lead (DSL) is responsible for online safety, this is supported by the Deputy DSLs and computing leads.

Aims

The policy identifies the measures in place in our school

- to protect children from undesirable content on the Internet
- to educate children about online safety issues including content, contact, conduct and commerce
- to protect them from undesirable contacts over the Internet
- to prevent unacceptable use of the Internet by children or adults
- to address issues of copyright for materials published on the Internet

Internet Access

- The school has a duty to provide children with quality internet access as part of their learning experience.
- The internet is an essential element in 21st century life for education, business and social interaction.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children.
- Internet use can enhance learning.
- Safe use of the internet will be taught discretely and alongside internet use for other subjects where appropriate.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of children (as provided by the SWGfL). Settings are protected by Group Policy via the server.
- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Children will be taught how to evaluate internet content.
- Children will be taught appropriate online conduct.
- The school will ensure that the use of internet derived materials by staff and children complies with copyright law.
- Children will be taught the importance of cross-checking information before accepting its accuracy.
- Children will be taught the importance of password privacy. Passwords will be reset annually, or sooner if the need arises.
- Children will be taught how to report unpleasant internet content.
- Staff are expected to adhere to the current internet safety guidelines as stated by the SWGfL (see appendices)
- Children must immediately tell a teacher if they receive an offensive online communication at school.
- In online communications, children must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online are for the schools' offices.
- The Executive Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs will be carefully selected for use on the website and only used if parents/carers have not withdrawn permission in writing.
- Full children' names will not be used in association with photographs anywhere on the school Web site or other on-line space.
- Parents permission will be sought on photos, videos and publishing on the school admission form.

Social networking and personal publishing

- Social networking sites are not permitted for use in school.
- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged children. Children will be taught about e-safety and information shared with parents through the newsletter and website.
- Children will be advised never to give out personal details of any kind that may identify them, their friends or their location.
- Seesaw is used as a secure communication tool between school and families.

Managing video conferencing & webcam use

- When available, video conferencing and webcam use will be appropriately supervised for the children' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones belonging to children will not normally be allowed in the classroom. For junior children they may be brought to school, but will be kept in the school office during the school day.
- Games machines may not be used in school.
- Smart watches with recorded capability may not be worn in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to General Data Protection Regulation.

Procedures (including Filtering and Monitoring)

- Anti-virus software operates on demand and automatically on a daily schedule.
- Disaster recovery for the schools' administration servers is via daily back up with the cassette removed from the premises.
- There are three standard levels of security, child, staff and admin. These are set by the schools technical support.
- The list of authorised users is reviewed annually by the admin teams.
- Acceptable use posters will be displayed in rooms where internet access is available.
- All staff will use encrypted storage devices or school laptops only for any documents containing data about the children.
- The school will work in partnership with parents, the LA, DfE and the SWGfL (South West Grid for Learning) to ensure systems to protect children are reviewed and improved. This will occur in response to the launch of new systems or procedures by the external agencies listed, or every three years, whichever is sooner.
- The senior leaders will ensure that standards for filtering and monitoring are met and will review this provision at least annually to ensure that it meets the schools' needs and record their findings.
- If staff or children discover unsuitable sites, the URL (address) and content must be reported to a member of the welfare and safeguarding team (WaST) and to SWGfL via the schools' admin

team. The Executive Headteacher will be informed.

- Any concerns about the suitability of sites will be reported to SWGfL by the admin teams. A log will be kept in school showing the site and the action taken. Any unsuitable sites will be placed on the schools' blocked lists.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The schools cannot accept liability for any material accessed, or any consequences of internet access.
- E-Safety training will be embedded within the computing scheme of work. Elements will also be covered within the Personal Social and Health Education (PSHE) curriculum if relevant.
- Staff will always use a suitable and safe search engine when accessing the web with children.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff will have individual log-ins and passwords. Children will have a class or group log in at the infant school and a personal log in at the junior school.
- The senior leadership team will look at a random sample of devices and internet traffic linked to an individual account to monitor acceptable use.
- Staff will minimise safeguarding risks which may occur from internet use by monitoring children's screens during sessions by roaming around the classroom during the lesson or using live supervision, e.g. children casting their screens onto the smartboard.
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone.
- Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.
- Staff must only use mobile phones during teaching time in emergencies. They must not use camera phones within the school day. This also applies when carrying out a school activity that occurs at another time.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with partnership safeguarding procedures.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the school E-Safety Policy annually when agreeing the acceptable use policies.
- The school will ask all parents and children to sign the acceptable use policy for children on admittance to the school.

Rules for Acceptable Internet Use

- The school has computers, ipads and internet access to help our learning.
- The following rules will help us keep everyone safe and help us be fair to others.
- These rules are laid out in the Acceptable Use Policy for children and the Acceptable Use Policy for staff which are in the appendix of this policy.
- This Acceptable Use Policy for children will be displayed on the iPad and laptop storage trolleys and cabinets in each school. Families will be provided with a copy of the relevant Acceptable Use Policy Agreement on joining the school.

This policy should be read alongside policies for:

- Anti-bullying
- Equalities
- SEND

- Safeguarding
- Whistle Blowing
- Complaints
- Data protection and Freedom of Information

This policy has been reviewed collectively by the staff and governors. It will be revised regularly in line with the school's rolling programme for policy review.

September 2023



Innsworth Infant School
Innsworth Schools' Partnership

Pupil Acceptable Use Policy Agreement (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the iPads
- I will only use activities that a teacher or suitable adult has suggested or allowed me to use.
- I will take care of the iPads and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think something is wrong.
- I will tell a teacher or suitable adult if I see something that I am unsure of on the screen
- I know that if I break the rules I might not be allowed to use the iPads

I have read and understood the school Acceptable Use Agreement.

Signed (child):.....

Signed (parent):

This agreement is based on advice from

SOUTH WEST
GRID
FOR LEARNING



Innsworth Junior School
Innsworth Schools' Partnership

Pupil Acceptable Use Policy Agreement (KS2)

These rules will help keep me safe when using ICT:

- I will ask an adult before I use computer equipment/internet or iPads
- I will only use activities that an adult has told me to use
- I will take care of computers and other computing equipment
- I will tell a teacher or suitable adult if I receive a message or see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer or iPad
- I will only edit and delete my own files and not look at, or change, other people's files without their permission
- I will keep my logins and passwords safe
- I am aware that some websites and social networks have age restrictions and I will respect this
- I will only message people I know, or who have been approved by a responsible adult
- Any messages I send or information I upload will always be polite and sensible
- I will not open attachments or files unless I know and trust the person who has sent it
- I will not give out my home/school address, phone number, photographs or other personal information unless a trusted adult has given permission
- I will never arrange to meet someone I have never previously met unless my parent/carer has given me permission and a responsible adult is with me

I have read and understood the school Acceptable Use Agreement.

Signed (child):.....

Signed (parent):

This agreement is based on advice from

SOUTH WEST
GRID
FOR LEARNING



Innsworth Schools' Partnership Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that partnership systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- The partnership will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for children's 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that children receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the partnership will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, ipads etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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 partnership.
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 partnership 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 partnership's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the schools' websites) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use personal social networking sites in school.
- I will only communicate with students / children and parents / carers using official school systems. 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 partnership and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schools:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using partnership equipment. I will also follow any additional rules set by the partnership about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use my mobile phone to contact parents and will keep my personal contact information confidential.
- I will not use personal email addresses on the partnership ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant procedures.
- 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 or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) 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 programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without the permission of a member of the SLT.
- I will not disable or cause any damage to partnership equipment, or the equipment belonging to others.
- I will ensure that where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- 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 partnership 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 the schools:

- I understand that this Acceptable Use Policy applies not only to my work and use of partnership digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the partnership.
- I will ensure appropriate privacy settings on my personal social media and be mindful of my professional status.
- 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 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 digital technology 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.

Staff / Volunteer Name:

Signed:

Date:

This policy is modelled on the template created by SWGfL