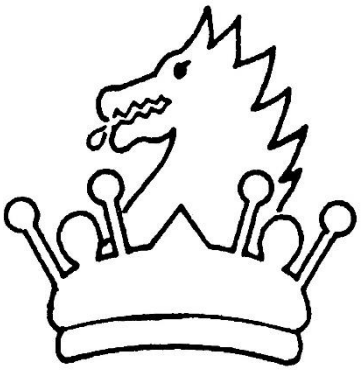
ICT and internet acceptable use policy

Willersey C of E Primary School



December 2021

Willersey C of E Primary School E-S AFETY AND ACCEPTABLE USE

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective E-Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our E-Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

VISION:

The use of computers is an important resource to support learning and teaching, as well as playing a significant role in the everyday lives of children, young people and adults. Schools need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment. Willersey C of E Primary School aims to provide a diverse, balanced and relevant approach to the use of technology that gives our pupils both the skills and wisdom to use it to best effect.

We aim to:

- Through a variety of media encourage the children to maximise the benefits and opportunities that technology has to offer.

- Ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

- Equip our pupils with the skills and knowledge to use technology appropriately and responsibly.

- Recognise the risks associated with technology and how to deal with them, both within and outside the school environment

- Ensure the users in the school community understand why there is a need for an E-Safety Policy.

THE ROLE OF THE ES AFETY CO-ORDINATOR

The role of the E-Safety Co-ordinator includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's E-Safety Policy and associated documents, including Acceptable Use Policies.

- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an E-Safety incident occur.

• Keeping personally up-to-date with E-Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).

• Providing or arranging E-Safety advice/training for staff, parents/carers and governors.

• Ensuring the head teacher, staff, pupils and Governors are updated as necessary. At Willersey C of E Primary School the E-Safety Co-ordinator is the Headteacher and ICT Lead.

POLICIES AND PRACTIC E SECURITY AND DAT A MAN AGEMENT

In line with the requirements of the Data Protection Act (1998) and the GDPR legislation (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

• Accurate

• Secure

• Fairly and lawfully processed

• Processed for limited purposes

• Processed in accordance with the data subject's rights

• Adequate, relevant and not excessive

• Kept no longer than is necessary

• Only transferred to others with adequate protection

• All laptops are password protected All data in the school is kept secure and staff informed of what they can or can't do with data through the E-Safety Policy and statements in the Acceptable Use document.

• The Senior Leadership Team are responsible for managing information.

• Staff are aware of where data is located.

• All staff with access to personal data understand their responsibilities.

• The school ensures that data is appropriately managed both within and outside the school environment.

• The staff are aware that they should only use approved means to access, store and dispose of confidential data.

• Staff have access to school logins, to ensure the data remains secure.

• The school's policy on using mobile devices and removable media is that school information is not allowed to be carried on unencrypted pen drives and no school data is allowed to be removed out of

school on removable devices unless password protected. It is preferable for staff to use password protected drive storage.

- The school aims to ensure that data loss is managed by the use of passwords for the required people.

- The school's procedure for backing up data is to use the internal server and XXXXXXX.

USE OF MOBILE DEVICES

Mobile phones are not encouraged to be brought into school by children. Should parents feel their child has a need to bring a phone into school they need explain that need to school staff. If a phone is brought in by mistake or is needed after school it is stored in the school office.

USE OF DIGITAL MEDI A

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites. To ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media, any images taken at school will only be used for school purposes e.g. website, brochure or display. In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- At school, photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (2018), and the school has written permission for their use from the individual and/or their parents or carers.

- The school seeks consent from the pupil, parent/carer or member of staff who appears in the media or whose name is used.

- The parental/carer permission is obtained on entry to school but parents have a right to change this if deemed necessary.

- Parents/carers, who have been invited to attend school events are allowed to take videos and photographs if appropriate (videos are sometimes disallowed when the show is being recorded or when videoing by parents would cause inconvenience to others).

- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.

- The school ensures that photographs/videos taken by staff are only taken using school equipment and only for school purposes.

- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.

- Staff are not to store school digital content on personal equipment. The staff are not to use their own cameras or phones to take photographs of children.

• When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.

• Staff, parents/carers and pupils made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.

• The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the SLT and Governors on an annual basis.

COMMUNICATION TECHNOLOGIES

School uses a variety of communication technologies and is aware of the benefits and associated risks. Email All users have access to Microsoft 365 as the preferred school e-mail system.

• Only official email addresses are used between staff and with pupils/parents when personal/sensitive data is involved.

• The filtering service reduces the amount of spam (Junk Mail) received on school email accounts.

• All users are aware of the risks of accessing content including spam, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.

• All users are aware that email is covered by The Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

• All users are aware that all email communications may be monitored at any time in accordance with the E-Safety and Acceptable Use Policy.

• All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Social Networks Social Network sites allow users to be part of a virtual community. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' content, send messages and leave comments. All staff need to be aware of the following points:

• They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

• Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.

• If a Social Network site is used, details must not be shared with pupils and privacy settings be set at maximum.

• Neither pupils nor parents must ever be added as 'friends' on any Social Network site but exceptions may be made at the head teacher’s discretion.

• Staff should be aware that most social media networks have age restrictions in place and should make children and parents are of this if necessary. Remember; whatever means of communication

you use, you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever. Even if your profile appears anonymous (using nickname, maiden name etc), you are still an employee of Willersey C of E Primary School and anything you post, share or like can be viewed as representative of the Local Authority.

Mobile telephone

• The school allows personal mobile phones to be used in school by staff and visitors but are asked to be left on silent and out of site in curriculum and meeting time.

• It is acceptable to use personal mobile phones for school activities e.g. school trips.

• Mobile phones are not encouraged to be brought into school by children. Should parents feel their child has a need to bring a phone into school they need explain that need to school staff. If a phone is brought in by mistake or is needed after school, it is stored in the school office.

Instant Messaging

Instant Messaging is a popular communication tool with both adults and children. It provides an opportunity to communicate in 'real time' using text, sound and video. These sites are blocked by default, but access permissions can be changed at the request of the Head Teacher

• Willersey C of E Primary School will ensure that Staff and children are aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts. Websites and other online publications This may include for example, podcasts, videos, 'Making the News' and blogs.

• The school website is effective in communicating E-Safety messages to parents/carers.

• Everybody in the school is made aware of the guidance for the use of digital media on the website.
• Everybody in the school aware of the guidance regarding personal information on the website.

• Key members of staff have access to edit the school website.

• The Head teacher has overall responsibility for what appears on the website.

Video conferencing

Video conferencing has just been introduced at Willersey C of E Primary School.

• All involved in video conference must be appropriately dressed.

• People near to the video conference should be aware that it is taking place (e.g. parents should inform family members).

• No recording is to take place and no still images taken.

• Video conferencing should only take place using Microsoft Teams or School Cloud (for parents' evenings). Others The School will adapt/update the E-Safety and Acceptable Use Policy in light of

emerging new technologies and any issues or risks associated with these technologies e.g. Bluetooth and Infrared communication.

ACCEPTABLE USE

Our E-Safety and Acceptable Use Policy is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of computers for educational, personal and recreational purposes. AUPs are used for Staff and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school and made available to all staff.

Our school's E-Safety and Acceptable Use Policy aims to:

- Be understood by each individual user and relevant to their setting and purpose.

- Be regularly reviewed and updated.

- Be regularly communicated to all users, particularly when changes are made to the E-Safety and Acceptable Use Policy.

- Outline acceptable and unacceptable behaviour when using technologies, for example:

o Cyberbullying

o Inappropriate use of email, communication technologies and Social Network sites and any online content

o Acceptable behaviour when using school equipment /accessing the school network.

- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.

- Provide advice for users on how to report any failings in technical safeguards.

- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.

- Outline sanctions for unacceptable use and make all users aware of the sanctions.

- Stress the importance of E-Safety education and its practical implementation.

- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

DEALING WITH INCIDENTS

The Head Teacher is responsible for dealing with E-Safety incidents.

• Staff are aware of the different types of E-Safety incident (illegal and inappropriate) and how to respond appropriately.

• Children are informed of relevant procedures through discussions with members of staff.

• Incidents are logged by the Headteacher.

• The above mentioned E-Safety Incident Log is the responsibility of the Resources Committee.

• The head teacher will decide at which point parents or external agencies are involved Illegal offences. Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Staff should never personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Any potential illegal content would be reported to the Internet Watch Foundation. They are licensed to investigate - schools are not! Examples of illegal offences are:

• Accessing child sexual abuse images

• Accessing non-photographic child sexual abuse images

• Accessing criminally obscene adult content

• Incitement to racial hatred More details regarding these categories can be found on the IWF website. Inappropriate use It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions. Accidental access to inappropriate materials

• Minimise the webpage/ Turn the monitor off

• Tell a trusted adult.

• Persistent 'accidental' offenders may need further disciplinary action. Using other people's logins and passwords maliciously / Deliberate searching for inappropriate materials / Bringing inappropriate electronic files from home / Using chats and forums in an inappropriate way.

• Inform SLT or designated E-Safety co-ordinator.

• Enter the details in the Incident Log.

• Additional awareness raising of E-Safety issues and the AUP with individual child/class.

• More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.

• Consider parent/carer involvement.

INFRASTRUCTURE AND TECHNOLOGY

The school ensures that the infrastructure/network is as safe and secure as possible. Broadband connection, filtering and virus protection are provided by Focus Networks.

PUPIL ACCESS

The children are supervised by staff when accessing school equipment and online materials

PASSWORDS

• All staff users of the school network have a secure username and password.

• The administrator password for the school network is available to the Headteacher and other nominated senior leaders is kept in a secure place.

• Staff are reminded of the importance of keeping passwords secure

• Passwords will only be changed if the need arises.

SOFTWARE/HARDWARE

• The school has legal ownership of all software.

• The school has an up to date record of appropriate licences for all software and the Computing subject leader is responsible for maintaining this.

MAN AGING THE NETWORK AND TECHNICAL SUPPORT

• Servers, wireless systems and cabling are securely located and physical access restricted.

• The Head teacher and School Business Manager are responsible for managing the security of the school network.

• The safety and security of the school network is monitored on a regular basis.

• The school systems are kept up to date in terms of security e.g. computers are regularly updated with critical software updates/patches.

• Users (staff, pupils, guests) have clearly defined access rights to the school network e.g. they have a username and password.

• Staff and pupils are encouraged to lock or log out of a school system when a computer/digital device is left unattended.

• Only the administrator is allowed to download executable files and install software.

• Users report any suspicion or evidence of a breach of security to the SLT.

• The school encourages staff not to use removable storage devices on school equipment e.g. pen drives unless password protected. It is preferable to use drive storage.

• If network monitoring takes place, it is in accordance with the Data Protection Act (1998)

• All internal/external technical support providers are aware of your schools requirements /standards regarding E-Safety

• The SLT, Computing Lead or School Business Manager is responsible for liaising with the ICT Technician.

• If a school laptop is used at home around other members of the family, precaution must be taken to ensure data is not viewed. Family members should not use staff laptops.

FILTERING AND VIRUS PROTECTION

Willersey C of E Primary School uses a filtering system for school and regularly updates its virus software.

EDUCATION AND TRAINING

In 21st Century society, pupils need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond. The main areas of E-Safety risk that we need to consider:

ESAFETY ACROSS THE CURRICULUM It is vital that pupils are taught how to take a responsible approach to their own E-Safety. Willersey C of E Primary School provides suitable E-Safety education to all pupils:

• Regular, planned E-Safety teaching within a range of curriculum areas.

• E-Safety education is differentiated for pupils with special educational needs.

• Pupils are made aware of the impact of Cyber-bullying and how to seek help if they are affected by these issues.

• Pupils are taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions.

• The school ensures that pupils develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school.

• Pupils are reminded of safe Internet use e.g. classroom displays, E-Safety rules and acceptance of site policies when logging onto the school network .

• Pupils are taught to understand that not all information online is factual and can be open to interpretation, and that they should be wary of online content.

ESAFETY - RAISING STAFF AWARENESS

• All staff are regularly updated on their responsibilities as outlined in our school E-Safety and Acceptable Use Policy.

• The E-Safety Co-ordinator provides advice/guidance or training to individuals as and when required.

• The E-Safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.

• All staff are expected to promote and model responsible use of ICT and digital resources.

• E-Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's E-Safety and Acceptable Use Policy.

• Regular updates on E-Safety and Acceptable Use Policy, curriculum resources and general E-Safety issues are discussed in staff/team meetings.

ESAFETY - RAISING PARENTS/C ARERS AW ARENESS

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. Byron Report, 2008 The school offers opportunities for parents/carers and the wider community to be informed about E-Safety, including the benefits and risks of using various technologies. For example through:

• School newsletters, homework diaries, Website,.

• Promotion of external E-Safety resources/online materials.

ESAFETY - RAISING GOVERNORS' AWARENESS

The school ensures that Governors, particularly those with specific responsibilities for E-Safety, ICT or child protection, are kept up to date on matters relating to E-Safety. The E-Safety and Acceptable Use Policy will be reviewed yearly (and/or if a serious breach occurs) by the E-Safety coordinator, approved by the governing body and made available on the school's website.

STANDARDS AND INSPEC TION

Since September 2009 there has been greater emphasis on monitoring safeguarding procedures throughout schools. At Willersey C of E Primary School:

• E-Safety incidents are monitored, recorded and reviewed.

- The Head Teacher is responsible for monitoring, recording and reviewing incidents.

- The introduction of new technologies is risk assessed and these assessments are included in the E-Safety and Acceptable Use Policy as appropriate.

Willersey C of E Primary School Acceptable Use Agreement:

STAFF

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed "reasonable" by the Head or Governing Body.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will not have any pupil or parent as a 'friend' on any social network platform unless agreed with the headteacher.

- I am aware that I represent the Local Authority in everything that I post, share or like on social networks.

- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body and only on password protected devices.

- I will not install any hardware or software without seeking permission from the Headteacher.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- I will not take photographs of pupils with any personal device e.g. mobile phone or camera.

- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will support and promote the school's e-Safety and Acceptable Use Policy.

- I will take responsibility for the contents of any shared or forwarded emails or social media posts and will ensure that their content (including attached comments) adheres to the E-Safety and Acceptable Use Policy.

Acceptable Use Agreement / ESafety Rules:

PUPILS

- I will only use ICT in school for school purposes.
- I will only use the school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my ESafety.

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.

Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous.

Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate.

Someone online may not be telling the truth about who they are - they may not be a 'friend.'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.