



Windmill Hill Primary School

Online Safety & Acceptable Use Policy

Online Safety Policy

Responsibilities

The member of school staff responsible for online safety is Paula Newman (Headteacher). She is responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote online safety within the school community. She may also be required to deliver workshops for parents.

The school Online Safety Policy aims to protect children from potentially harmful and inappropriate online material. The four main areas of concern are:

Content – children being exposed to illegal, inappropriate, or harmful content, for example pornography or fake news.

Contact – children being subject to harmful online interactions with other users, for example, adults posing as other children with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct – online behaviour that increases the likelihood of, or causes harm, for example, sending or receiving explicit images of other children or online bullying.

Commerce – online risks such as gambling or online advertising.

Children will be taught about how to recognise and respond to concerns when online through the school curriculum.

Internet use and Acceptable Use Policies (AUPs)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role.

Examples of the AUPS used can be found in Appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip.

This can be found in Appendix 2.

AUP's will be reviewed annually. All AUPs will be stored centrally in case of breaches of the Online Safety Policy.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's computing curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff members have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images. Consent is requested when the child starts school and amended when necessary.

Staff should always use a school electronic device to capture images and should not use their personal devices. Photos taken by the school are subject to the Data Protection Act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see Appendix 2).

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

Windmill Hill Primary School recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.

The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

Windmill Hill Primary School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in spaces where the children are present. If staff members fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. Staff must ensure that there is no inappropriate or illegal content on the device.

There may be occasions in school when it is necessary for a member of staff to use their personal mobile phone for work related purposes, for example, to sign into online recording systems an authenticator app is required or Class Dojo. In these situations, the rationale for using the mobile phone must be given to the Headteacher. The Headteacher will consider the information provided and either give the member of staff permission to use the mobile phone or decline permission for the member of staff to use the mobile phone.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit, volunteers and visitors are given a leaflet explaining safeguarding expectations. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

Important contact details of the children are kept on the schools mobile phone in case of an emergency.

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails

Pupils should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked'). All users should be aware that the ICT system is filtered and monitored.

Data storage

Only USB pens that are password protected are to be used in school.

Reporting

All breaches of the Online Safety Policy need to be recorded.

In the event of a breach of the Online Safety Policy, or when there are concerns that a child may have an electronic device in school containing inappropriate or illegal information or images, the school will follow the guidance provided in "Searching, Screening and Confiscation" (2022) in order to ensure the safety and wellbeing of all involved. This may include confiscating electronic devices.

Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to Miss Newman in the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, ChildLine).

Infringements and sanctions

Whenever a student infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Level 1 infringements:-

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone]

Level 2 infringements:-

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Unauthorised use of mobile phone (or other new technologies)
- Continued use of unauthorised instant messaging / social networking sites
- Use of File sharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent]

Level 3 infringements:-

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act.
- Bringing the school name into disrepute.
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence.

Social networking

Pupils are not permitted to use social networking sites within school.

Online Education

Pupils

To equip pupils as confident and safe users of computing the school will undertake to provide:

- a) A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- b) Regularly auditing, review and revision of the computing curriculum.
- c) Online safety resources that are varied and appropriate and use new technologies to deliver online safety messages in an engaging and relevant manner.
- d) Opportunities for pupils to be involved in online safety education e.g. through peer mentoring, online safety committee, parent presentations etc.

Additionally,

- a) Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- b) There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- c) The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour.
- d) Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

- a) A planned programme of formal online safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
- b) Online safety training is an integral part of Child Protection / safeguarding training and vice versa.
- c) All staff have an up to date awareness of online safety matters, the current school online safety policy and practices and child protection / safeguarding procedures.
- d) All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policy.
- e) Staff are encouraged to undertake additional online safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate

- f) The culture of the school ensures that staff support each other in sharing knowledge and good practice about online safety.
- a) The school takes every opportunity to research and understand good practice that is taking place in other schools
- b) Governors are offered the opportunity to undertake training.

Parents and the wider community

The class teacher will keep parents informed of the websites that children are asked to access at home for the purpose of homework and will also be informed of what children are being asked to do online. If, at any time, a member of staff will be interacting with pupils online, we will always inform parents in advance and will inform parents of the name of the person who will be interacting with their child online along with the reason for the online contact.

Online Safety apps are available on the school website to ensure that all members of the school community are up to date with the current advice on how to keep children safe when online.

Filtering, Monitoring and reporting

- a) The school network provides a level of filtering and monitoring that supports safeguarding.
- b) In order to ensure the safety of all members of the school community, anytime an inappropriate search is made through the school network, an alert is sent to the headteacher. Safeguarding procedures would then be followed.
- c) The school action plan indicates any planned action based on the above.

Adopted by the Governors June 2025

Appendices

Appendix 1 – Acceptable Use Policies

Acceptable Use Policy for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

Signed

Name

Date

Acceptable Use Policy for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

I know that anything I share online may be monitored.

I know that once I share anything online, it is completely out of my control and may be used by others in a way that I did not intend.

Signed

Name

Date

Acceptable Use Policy for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

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 images
 - promoting discrimination of any kind
 - promoting violence or bullying
 - promoting racial or religious hatred
 - promoting illegal acts
 - breach any Local Authority/School policies on the school premises
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

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

Signed

Name

Date

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a designated governor for safeguarding takes responsibility for e-Safety
- an e-Safety Policy has been written by the school
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

Windmill Hill Primary School

Parent / Guardian Name:

Pupil Name:

Pupil's Registration Class:

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service; secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent / Guardians' Signature:

Your Name (in block capitals)

Date

Appendix 3 – School Audit

Audit

The self-audit should be completed by the member of the Management Team responsible for the e-Safety Policy.

Is there a school e-Safety Policy that complies with Halton guidance?	Yes
Date of latest update (at least annual):	June 2024

Appendix 4 – Photo/video consent

School Name:

Pupil Name:

Pupil's Registration Class:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.

To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please bring the completed form to school. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

1. May we use your child's image in our printed promotional publications? Yes / No
2. May we use your child's image on the school website/SLG? Yes / No
3. May we record your child's image on our promotional videos? Yes / No
4. May we use your child's image in the local press? Yes / No

Parent / Guardians' Signature:

Your Name (in block capitals)

Date