New Scotland Hill Primary School and Nursery

Enjoying living and learning together

E-SAFETY POLICY

Date published	December 2024
Version	V4
Date for review	December 2026

New Scotland Hill School
E-Safety Policy V3

Introduction
We recognise the part that the internet plays in the lives of everyone and is seen as an important life-skill and is vital to access life-long learning and employment. We recognise that the internet provides many benefits, not just to children, young people and vulnerable adults, but also to the professional work of staff.

A glossary of terms is included in Appendix i.

Definition
E-safety is defined as being safe from risks to personal safety and well-being when using all fixed and mobile devices that allow access to the internet as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles.

Safeguarding against these risks is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

It is not possible to create a 100% safe environment and it is our school's responsibility to demonstrate that we have managed the risks and do everything we reasonably can to protect the children, young people or vulnerable adults that they work with.

Aims
We aim to:

- Audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- Ensure that children, young people and vulnerable adults are educated about what they read, hear and see on the internet
- Work closely with families to help them ensure that their children use new technologies safely both at home and in school
- Provide an age appropriate, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies (see Appendix ii)

Acceptable Use Policy (AUP)
All organisations providing internet access for children, young people and vulnerable adults should have AUPs in place which set out guidance for the acceptable, safe and responsible use of on-line technologies. The correct and appropriate use of AUPs will safeguard not only those that are vulnerable but also adults who work or volunteer within these settings. This document is included in the staff induction pack and in the volunteers information pack. Our agreed AUP can found in Appendix iii.

E-safety Leader
This is the responsibility of the Headteacher.
The e-safety Leader is responsible for:

- Maintaining the AUPs
- Ensuring that the organisation's policies and procedures include aspects of e-safety
- Working with the filter system provider to ensure that the filtering is set at the correct level for staff, children, young people and vulnerable adults
- Ensuring that staff participate in e-safety training
- Ensuring that e-safety is included in staff induction
- Monitoring and evaluating incidents that occur to inform future safeguarding developments

Managing Incidents
The Headteacher will ensure that these procedures are followed in the event of any misuse of the internet:

Inappropriate contact
1. Report to the Headteacher
2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence
3. Contact the parent(s)/carer(s)
4. Contact the police on 101
5. Log the incident
6. Identify support for the child, young person or vulnerable adult

Cyber-bullying
1. Report to the Headteacher
2. Advise the child, young person or vulnerable adult not to respond to the message
3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the parent(s)/carer(s)
6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence
7. Log the incident
8. Identify support for the child, young person or vulnerable adult

Malicious or threatening comments
1. Report to the Headteacher
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
4. Inform and request that the comments are removed from the site/block the sender
5. Inform the police on 101 as appropriate
6. Log the incident
7. Identify support for the child, young person or vulnerable adult

Inappropriate viewing of materials
1. Report to the Headteacher
2. If illegal, do not log off the computer but minimise the screen or turn the screen off
3. Record the website address as well as the date and time of access
4. If appropriate, refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message
5. Decide on the appropriate sanction
6. Inform the parent(s)/carer(s)
7. Contact the filtering software provider to notify them of the website
8. Log the incident
9. Identify support for the child, young person or vulnerable adult

Allegations against a member of staff

In the case of the above, the school's policy on Child Protection and the Berkshire LSCB Child Protection Procedures should be referred to https://berks.trixonline.co.uk/

All allegations should be reported to the organisation manager, police (101) and the Local Authority Designated Officer (LADO) (01344 352020), as appropriate.

Appendix i

Glossary of terms

Cyberbullying: Bullying using technology such as computers and mobile phones

Frape: Short for "Facebook rape", referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset

Grooming: This is defined by the UK Home Office as: "a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the contact would be for unlawful purposes".

Hacker: Originally thought of as a computer enthusiast, but now a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.

Locked down system: In a locked down system, almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe because they can only use websites vetted by their teachers, the technicians or by the local authority. This does not encourage pupils to take responsibility for their actions.

Managed system: In a managed system, the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools with managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are give the opportunity to learn how to assess and manage risk for themselves.

Phishing: This is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the emails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen.

Appendix ii

ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

e-safety Rules

Ask permission before using the internet

Tell a trusted adult if you see anything that makes you feel uncomfortable

Immediately close any webpage that you are uncomfortable with

Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details

Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos

Only contact people that you have actually met in the real world

Never arrange to meet someone that you have only met on the internet

Only use a webcam with people you know

Think very carefully about any pictures that you post online

Only open e-mails from people that you know

Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as http://www.askforkids.com

This page has been developed by the e-safety sub-group of the Bracknell Forest Local Safeguarding Children Board (LSCB). For more information contact the e-safety Lead Officer on 01344 352000.

Appendix iii

Acceptable Use Policy Agreement (Staff)

Technology is now entwined in our modern lives with everyday use of social media and web-based communication a standard practice. It is therefore important to ensure good awareness both of the possibilities to learn, create and share ideas and also the risks that these freedoms bring both to the welfare of staff and students and to the integrity of the IT systems that the school relies on to provide learning and teaching.

All users access our school systems should are entitled to safe access to the internet and IT systems at all times. This policy is intended to provide a working framework for staff to uphold the positive ideals of the technology we use while providing a safe learning environment and protecting the data we manage in the course of our services to students and their families.

The policy will outline how:

- Staff must ensure they are responsible users of the IT systems provided and that they make sound judgements while using the internet and other communications technologies for educational and personal use.
- The school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff can ensure they are protected from potential risk in their use of technology for educational and personal use.

Schools AUP Agreement:

I agree that I must use school IT systems in a responsible way. I must do so to ensure there is no risk either to my own safety or to the safety and security of the students and school IT systems. I will, where possible, guide students in the safe use of technology with a strong focus on safe and responsible use of the internet and online services.

For the purposes of safeguarding and security:

- I understand that the school will monitor my use of the school IT and communications systems.
- I understand the rules in this document apply equally to the use of school and personal devices and systems (e.g. laptops, email, VLE etc.) outside of school
- I understand the importance of appropriate controls on the transfer and sharing of personal data (digital or paper-based) out of school.
- I understand that the school IT systems are primarily intended for educational use.
- I will only use the systems for personal or recreational use when appropriate.

Acceptable Use Policy: Staff

- I will never disclose my username or password to anyone else, nor use any other person's username and password to access systems not provided to me.
- I understand that I should not record any password where it is possible that someone may view it or steal it.
- I will immediately report any incident or activity I am aware of which may be illegal, inappropriate or present risk to the school or individuals to the Head teacher.

I will use all the school IT and communication systems professionally. In doing so:

- I will not access, copy, alter, share or delete any other user's files, without their express permission.
- I will communicate with others in a professional manner and refrain from any use of aggressive or inappropriate language.
- I will ensure that, if I wish to take or publish images of others I will check that appropriate consent is recorded by the school in lines with the school's digital media policy.
- I will only use school provided and managed equipment to record these images unless I have explicit permission to do otherwise from the Headteacher.
- I will ensure that any published photos do not identify individuals by name or show other personal information and that photos and images are only used on a school approved and controlled platform.
- I will only use social networking services in school unless I have explicit permission to do otherwise from the Headteacher . At all times use must be in accordance with the school's policies.
- I will only communicate with students and parents/carers using provided school IT systems unless I have explicit permission to do otherwise from the head teacher (eg using personal device for social media) . All communication will be professional in tone and manner.
- I will wherever possible use the school provided and managed equipment to record any Safeguarding concerns on the CPOMS system . Where it is not possible to access school managed equipment in a timely manner then a personal device can be used. In both circumstances inputting onto CPOMS should only be undertaken in non-teaching areas of the school such as the staff room.
- I will ensure that I do not share my personal contact information and only ever use contact details provided by the school.
- I will not engage in any online activity that may compromise my professional integrity or provide a risk to the students, my colleagues, the school IT systems or myself.

The school and the local authority will provide safe and secure access to school IT systems and services and maintain the availability and integrity of the school systems in support of learning and teaching. However, any use of personal mobile devices (such as but not limited to, laptops/tablets/ mobile phones) in school, must be in accordance with rules set out in this agreement, as per any school managed equipment.

Staff members must:

- Ensure that any such personal devices are protected by up to date security patches and anti-virus software and are free from viruses.
- Remain vigilant when accessing emails. Never click on any hyperlinks in emails or any attachments to emails, unless the sender is known and trusted.
- Any concerns about emails or communication received on any other school or personal IT system must be flagged to the Head teacher
- All professional work must be stored in the appropriate, provided, locations on the school network or systems to guarantee appropriate levels of backup and malware scanning.
- Staff 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.
- Staff will not try to use any applications, such as VPN, that might allow them to bypass the filtering/security systems in place to provide a safe learning and teaching environment.
- Staff should not install any applications on school devices without consultation and support from the IT Manager. Neither should they change settings put in place by the school to ensure appropriately managed devices.
- Must report any damage to or faults in school equipment to the IT Manager.
- Will only share personal information collected and managed by the school with others as their role permits or when required by law or by school policy to disclose such information to an appropriate authority. Any data sharing must be by approved and encrypted communication services provide by the school or their business partners.
- Staff must ensure that copyright resources are only used or shared with appropriate permissions. Copyrighted work will not be downloaded or shared including music and videos unless an exemption applies for teaching purposes.
  These purposes include:
    - the copying of works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes, it is accompanied by a sufficient acknowledgement, and the use is fair dealing. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but uses which would undermine sales of teaching materials are not;
    - performing, playing or showing copyright works in a school, university or another educational establishment for educational purposes. However, it only applies if the audience is limited to teachers, pupils and others directly connected with the activities of the establishment. It will not generally apply if parents are in the audience. Examples of this are showing a video for English or drama lessons and the teaching of music. It is unlikely to include the playing of a video during a wet playtime purely to amuse the children;
    - by recording a TV programme or radio broadcast for non-commercial educational purposes in an educational establishment, provided there is no licensing scheme in place. Generally, a licence will be required from the Educational Recording Agency;
    - making copies by using a photocopier, or similar device on behalf of an educational establishment for the purpose of non-commercial instruction provided that there is no licensing scheme in place. Generally, a licence will be required from the Copyright Licensing Agency.

These and other, exemptions to copyright are listed here:
https://www.gov.uk/guidance/exceptions-to-copyright

I have read and understood the above and agree that:

- I am responsibly upholding the requirements laid out above at all times and that even while in personal time I am representing the values and integrity of the school.
- This Acceptable Use Policy applies not only to my work and use of school-provided IT equipment but also applies to my use of school IT systems on personal equipment both at school and on other private or public networks.
- If I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action as per the terms laid out in the school's Disciplinary Policy.

Name:	
Signed:	
Date:	