Highfields Primary School

E – Safety Policy

Written By: H Plant
Last Reviewed: April 2023
Adopted by Governors:
Next Review: April 2025

1. Rationale

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the real world. Increasingly, children are accessing material through the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy, supported by the Acceptable Use Policies (AUP; see appendices) for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: child protection, digital images, health and safety, behaviour and PSHE.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, voting systems, digital video equipment, etc) and technologies owned by pupils or staff.

2. The Technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant Messaging
- Blogs
- Social Networking Sites
- Chat Rooms
- Gaming Sites
- Text Messaging and Picture Messaging
- Video Calls
- Online Communities Via Games Consoles

3. Whole School Approach To The Safe Use Of ICT

Creating a safe Computing learning environment includes three main elements at this school:

- An effective range of technological tools which are filtered and monitored.
- Policies and procedures, with clear roles and responsibilities.
- A comprehensive E-Safety education programme for pupils.

4. Staff Responsibilities:

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy is monitored. All staff are encouraged to create a talking culture in order to address any E-

Safety issues which may arise in classrooms on a daily basis. All visitors also receive our acceptable use policy on arrival at school (from the school office). Copies of signed acceptable use policies can be obtained from the school office, when needed.

The responsibility for E-Safety has been designated to a member of the teaching staff.

Our school **E-Safety Co-ordinator** is Mrs H Plant.

Our E-Safety Coordinator ensures they keep up to date with E-Safety issues and guidance through liaison with SIPS Ltd E-Safety Officer (Sue Courtney – Donovan) and through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 degree safe. The school's E-Safety Coordinator ensures the Head, senior management and governors are updated as necessary.

Staff Awareness

- All staff receive regular information and training on E-Safety issues in the form of in-house training and meeting time when needed.
- New staff receive information on the school's AUP as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-Safety records of concern are recorded on CPOMS and are completed by staff as soon as incidents occur. They are reported directly to the school's designated safeguarding team - Mrs Sarah Garratt, Mrs Maria Lewis, Mrs Sian Evans and Mrs Elaine Adams.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school E-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Internet:

- Highfields will use Trustnet's 'filtered' Internet Service, which will minimise the chances of pupils encountering undesirable material.
- Staff, pupils and visitors have access to the internet through the school's fixed and mobile internet technology.
- Staff should email school-related information using their Office 365 address and not personal accounts.
- Staff will preview any websites before recommending to pupils.
- Suitable websites will be provided on class pages by staff for children to use.
- The CEOP Report Abuse button is available on the school website. Teachers make children aware of this and when it is appropriate to use it.
- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the Computing technician. This will then be reported to Trustnet and blocked as necessary.
- Staff and pupils are aware that school-based email and internet activity is monitored and can be explored further if required.
- Pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider (Trustnet) or technician can block further access to the site.
- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved.
- They are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone should be made, unless this is part of an approved school project and parental consent has been given.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behavior policy.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile Technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- Mobile technology for pupil use, such as iPads and netbooks, are stored in a locked cupboard. Access is available via the school office key holders. Members of school staff (not visitors or children) should sign in/out the technologies before and after each use.
- No personal devices belonging to children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times only and kept on silent. If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept switched off and sent to the office during the day. Any children not following these rules will be dealt with using the school's behaviour policy.

Data Storage:

- Encrypt all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- No sensitive data should be stored on staff laptops (such as photos, IPPs and pupil information).
- IPPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by school, or on our secure Office 365 learning platform in the staff area.
- If any sensitive information is taken offsite, it must be stored on a password protected, encrypted USB memory stick.

Social Networking Sites:

- Use such sites with extreme caution, being aware of the nature of what you are publishing online in relation to your professional position.
- Under no circumstances should present or past school pupils be added as friends.
- Staff should be mindful about what they put on social media sites (both photos and posts), ensuring that they maintain a level of professionalism at all times (especially if they are friends with friends of parents).
- Make sure that any profiles are kept private to eliminate the chances of information being leaked.
- Under no circumstances should any reference to pupil's name or work be made on any social network site.
- Under no circumstance should any images of school children be used on social networks, including images in the background of other images.
- Any photographs taken inside school should not make the school identifiable and should certainly not show any pupils.

Digital Images:

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal camera phones to store images of children.
- Ensure you are aware of the children whose parents/guardians have not given permission for their child's image to be used in school. An up-to-date list is kept in the school office. This is also given out to class teachers as needed.

- When using children's images for any school activity, they should not also be identified by their full name.
- This relates to the to the Digital Images policy.

Members of staff who repeatedly breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

5. Providing A Comprehensive E-Safety Education To Pupils and Parents

- All staff working with children must share a collective responsibility to provide E-Safety education to pupils and to promote E-Safety in their own actions.
- Formally, an E-Safety education is provided by the objectives contained in the Computing unit plans for every area of work for each year group. Even if E-Safety is not relevant to the area of Computing being taught, it is important to have this as a 'constant' in the Computing curriculum.
- Informally, a talking culture is encouraged in classrooms which allows E-Safety issues to be addressed as and when they arise.
- The Computing Subject Champion will lead an assembly (alongside the Digital Leaders) on Safer Internet Day, highlighting relevant E-Safety issues and promoting safe use of technologies.
- All classes will focus on E-Safety at least once per year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies.
- Staff will ensure children know to report abuse using the CEOP button widely available on many websites, or to speak to any member of staff, who will escalate the concern to the Computing Subject Champion with responsibility for E-Safety.
- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's Computing guidelines. (See Appendix)
- Children will be encouraged to educate parents through both classroom activities and homework-based activities when possible.

6. Complaints Procedure:

As with other areas of school, if a member of staff, a child or a parent/carer has a complaint or concern relating to E-Safety, then they will be considered and prompt action will be taken. Complaints should be addressed to the E-Safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of E-Safety concern will be recorded using a CPOMS and reported to the school's designated safeguarding team (as listed above), in accordance with school's child protection policy. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

7. Updating the Policy:

This policy will be updated again in April 2025.

Appendix

Highfields Primary School

Computing Acceptable use policy for pupils for use at home (H) and at school (S).

The school has installed computers and Internet access to help our learning.

These rules will keep us safe and help us to be fair to others.

- I will only use computers in school for school purposes. (S)
- I will ask permission from a member of staff before using the Internet and will only be online when an adult is in the room. (S)
- I will only use my login and password and never share these with others. (S) (H)
- I will ask permission before bringing in memory sticks or CD ROMs into school. (S)
- I will only open and delete my own files. (S)
- The messages I send will be polite and sensible. (S) (H)
- I will never give out my own or other people's name, address or phone number online. (S) (H)
- I will never upload any images of school activities to any social networking site. (S) (H)
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. (S) (H)
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away. (S) (H)
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my E-Safety. (S)

Pupil Signed:____________________ Date:____________

Name:____________________ Class:_____

Parent Signed:____________________ Date:____________

Name:____________________

Highfields Primary School

Computing Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from E-Safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anyone outside of school.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Headteacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time without pupils.
- **I will report any E-Safety concerns to the designated safeguarding officer immediately using the E-Safety Record of Concern.**
- **I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.**
- **I will support the school's E-Safety policy and help pupils to be safe and responsible in their use of technology.**

Signed: ______________________ Date: ______________

Data Security

Highfields Primary School

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-

Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the school.

Staff should only save sensitive data in the following secure formats: -

1. On the learning platform (Office 365)
2. On the Staff Share drive
3. On the encrypted USB memory stick provided. The only USB sticks that should be used to store any sensitive data are those provided, which are already encrypted, by the school.

This ensures that no legal action can be taken for lost data.

If you lose your encrypted memory stick or are unable to open it because of a password error, you must inform the ICT technician without delay. It is imperative that you do not share or write down your password. You may add a question prompt reminder when first accessing your memory stick, which can be used if you have forgotten your password. It is your responsibility to keep the data from your memory stick regularly backed up in another secure format, the best way to do this would be to use the Office 365 learning platform.

Failure to follow these guidelines will be treated seriously and could lead to disciplinary procedure.

H. Plant
April 2023

I understand the procedures and agree to follow them with immediate effect

Name ____________________

Signed____________________