Primary Online Safety Framework

Heyhouses C.E. Primary School,
St. Annes- on- Sea,
Lancashire

2018

Developing and Reviewing this Policy

This eSatefy Policy has been written as part of a consultation process involving the following people:

Alison Townsend, Elizabeth Hodgson, Tim Fish, Teachers and Governors

It has been approved by the Governors and will be monitored and reviewed as listed below:

Policy created: February 2018

Policy Reviewed: February 2019

The implementation of this policy will be monitored by Tim Fish.

This policy will be reviewed as appropriate by Tim Fish.

Approved by Mrs Elizabeth Hodgson Headteacher

Date: February 2018

Approved by the Governing body.

Date: February 2018

Introduction

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Twitter
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, most of the above, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Heyhouses CE Primary School we understand the responsibility to educate our pupils and staff on online issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Our school holds personal data on learners, staff and other people to help us conduct our day-to-day activities. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and

pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, digital video equipment, etc.; and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.)

Monitoring

The Computing subject leader, Headteacher or Deputy, Assistant Headteacher may inspect any computing equipment owned or leased by the School at any time without prior notice.

Senior Management and the Computing subject leader may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by Computing authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Senior Management members and ICT subject Leader.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher and the ICT subject leader.

Whole School Education.

Staff and Governors

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

- Makes regular training available to staff on e-safety issues and the school's e-safety education program

- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safety policy and the school's Acceptable Use Agreements.

Parents

This school

- Runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.

- Information leaflets; in school newsletters; on the school web site;

- Demonstrations, practical sessions held at school;

- Suggestions for safe Internet use at home;

- Provision of information about national support sites for parents.

Pupils

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To STOP and THINK before they CLICK
    - To develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - To be aware that the author of a web site / page may have a particular

bias or purpose and to develop skills to recognise what that may be;

- To know how to narrow down or refine a search;
- [For older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button

Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Heyhouses School E-Safety Rules.

Pupil Acceptable Use Agreement.

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child, understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

1. I will only use ICT in school for school purposes.
2. I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher. Only upper Junior children may bring a mobile phone to school. Phones will be turned off and stored securely by the teachers. (see appendix 1 for rules regarding children having a phone at school)
3. I will only use the Internet and/or online tools responsibly.
4. I will only use my class e-mail address when emailing.
5. I will not deliberately look for, save or send anything that could be unpleasant or nasty.
6. If I accidentally find anything inappropriate I will tell my teacher immediately.
7. I will not deliberately bring in inappropriate electronic materials from home.
8. I will not deliberately look for, or access inappropriate websites.
9. I will only communicate online with people a trusted adult has approved.
10. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
11. I will not give out my own, or others', details such as names, school passwords, phone numbers or home addresses.
12. I will not arrange to meet anyone that I have met online.
13. I will only open/delete my own files.
14. I will not attempt to download or install anything on to the school network without permission.
15. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
16. 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 online safety. This is in line with the school behaviour policy.

We have discussed this Acceptable Use Agreement and

…… [Print child's name] agrees to follow school's Online rules and to support the safe use of ICT at Heyhouses School.

Parent /Carer Name (Print)……

Parent /Carer (Signature) ……

Class…… Date……This AUA must be signed and returned before any access to the school system is allowed.

Appendix 1

The use of mobile phones and other personal devices by pupils in school will be decided by the school and covered in this policy. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy. School staff may confiscate a phone or device if they believe it is being used to contravene this policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation. Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequence.

ICT Acceptable Use Agreement (AUA)
Staff, Governors and Visitors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in keeping safe while Online, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms. (See Appendix 1)
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will adhere to the staff personal device policy e.g. mobile phones and tablets. (Appendix 2)
9. I will not install any hardware or software without the prior permission of the ICT Coordinator.
10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
11. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
12. I will report any known misuses of technology, including the unacceptable behaviours of others.
13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
19. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……

Date ……

Full Name …… (PRINT)

Position/Role ……

<u>Appendix 1</u>

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

<u>Appendix 2</u>

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances. (If needing to make a personal phone the member of staff needs to ask for class cover.)
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

ICT Acceptable Use Agreement (AUA)
Parents and Carers

ICT and the related technologies such as e-mail, the Internet (Social Networking Sites) and mobile devices are an integral part of our daily life. This agreement is designed to ensure that all parents and carers are aware of their individual responsibilities when using technology. All parents and carers are asked to sign this policy and adhere to it at all times. By working together we hope to develop the children's awareness and understanding of how to be safe and happy while using developing technologies. Any concerns or clarification should be discussed with the Headteacher.

Rules and Guidance

Parent's and carers:

1. Will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text (Online discussions) that could upset or offend any members of the school community.
2. Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety Acceptable Use Agreement form at the time of their child's entry to the school and review it on a regular basis.
3. Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
4. Parents / carers are specifically informed of e-safety incidents involving their child and given support where needed.
5. Support the school in promoting online safety and endorse the Parents' Acceptable Use agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.
6. Will adhere to the guidance for taking photographs and videos in school. (Appendix 1)
7. Will read, understand and promote the school Pupil Acceptable Use Agreement with their children.
8. To access the school website when possible for information on school life.
9. To consult with the school if they have any concerns about their children's use of technology.

We will seek advice from outside agencies if one of our pupil's parents and carers or staff receives communication that we consider is particularly disturbing or breaches our school policy.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Childs Name…….. Class ……

Signature ……

Full Name …… (PRINT) Date ……

Appendix 1

Guidance When Taking Photographs/Videos in School

While reviewing the schools Online Safety policy we discussed the taking of video and photographs by parents, carers and friends at school events such as the school plays, class assemblies, carol services or sports days.

The policy here at Heyhouses C.E. Primary School is to allow photographs/videos to be taken and enjoyed as part of the children's involvement in these activities. We recognise that photographs/videos are a valuable and precious reminder of those magical moments your child enjoys in school and we do not want to limit your opportunities to record these by introducing any kind of ban. However, for us to continue with this policy it is essential that our community work with us by following the guidance included in this letter.

When taking photographs/videos we would like to clarify a few points especially with relation to social media.

- Whenever possible limit your photographs and videos to include only your child.
- If you have photographs/video which include children other than your own or staff do not upload this on to any social media sites unless you have the express permission from that child's parent/guardian.
- If you put any photographs/video taken at school related events or activities on to social media sites such as Facebook, Twitter, YouTube, Snapchat, Instagram and WhatsApp etc. please do not put any reference to Heyhouses C.E. Primary School
- When posting text, photographs and/or video to social media sites do not make reference to children's names (unless they are your own children)

At times we have children in our community whose parents, for a variety of reasons, are sensitive to their image being posted to the social media community. Be aware that once a photograph/video or comment is posted on a site it is there permanently even when deleted or withdrawn

There are many magical moments that we enjoy sharing with you throughout the school year and the Governors remain committed to working with and trusting our school community to cooperate with this guidance. The guidance will be reviewed annually.

School ICT Infrastructure

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;

Provides highly restricted simulated environments for e-mail with Key Stage 1 pupils;

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date

- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LA-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language

Pupils:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.

- Year R/1 pupils are introduced to principles of e-mail.

- Pupils cannot receive external email

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:

    - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - That an e-mail is a form of publishing where the message should be clear, short and concise;
    - They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
    - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;

- That they should think carefully before sending any attachments;
- Embedding adverts is not allowed;
- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- Not to respond to malicious or threatening messages;
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;

Pupils sign the school Acceptable Use Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- All staff sign our Acceptable Use Agreement Form AUA to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: <e.g. Computing Subject Leader >
- The school web site complies with the statutory DfE guidelines for publications;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

Social networking

The staff and pupils follow the schools Acceptable Use Agreements with regard to social networking.

Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - staff,
    - governors,
    - pupils
    - parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a secure area on the school network to store pupil sensitive data and photographs

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after computers are idle for 15 minutes.

- We do not permit if any member of staff has to take any sensitive information off site.

- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.

- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.

- All servers are in lockable locations and managed by DBS-checked staff.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

- Paper based sensitive information is shredded, using cross cut shredder / collected by secure data disposal service.