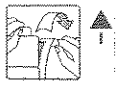
Ferham Primary School

E-Safety Policy

September 2018

Date agreed by Governors: Delegated to the Headteacher

Review date: September 2019

Policy for E-Safety

Contents:

Statement of Intent

At Ferham Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

1. Legal Framework

1.1 This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- **Regulation of Investigatory Powers Act 2000**
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Safeguarding Policy
- Anti Bullying policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks, which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games Loss of personal images
- Inappropriate communication with others Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside school, and to deal with incidents of such as a priority.

3.2. The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. The IT Technician and IT lead person (Sara Winder) is responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise.

3.4. The head teacher is responsible for ensuring that the IT Technician and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.5 The IT Technician and IT lead person will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.6 The head teacher will ensure there is a system in place, which monitors and supports the IT Technician and IT lead person, whose role is to carry out the monitoring of e-safety in school, keeping in mind data protection requirements.

3.7 The IT lead person will regularly monitor the provision of e-safety in the school and will provide feedback to the head teacher.

3.8 The head teacher has established a procedure for reporting incidents and inappropriate internet use, either by pupils or staff (CPOMS).

3.9 The IT lead person will ensure that all members of staff are aware of the procedure when reporting e-safety incidents.

3.10 The IT Technician will attempt to find alternatives to monitoring staff use of social media, where possible, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy. The member of staff who is being monitored will be consulted prior to any interception by the school.

3.11 Cyber bullying incidents will be reported in accordance with the school's Anti Bullying Policy.

3.12 The governing body will hold regular meetings with the head teacher to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

3.13 The head teacher and IT lead person will evaluate and review this E-Safety Policy on a regular basis, taking into account the latest developments in ICT and the feedback from staff/pupils.

3.14 The head teacher and IT lead person will review and amend this policy with the IT Technician, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.15 Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.16 All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

3.17 All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the head teacher.

3.18 Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.19 The IT lead person and PSHE lead are responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.20 All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. Educating staff:

- A planned calendar programme of e-safety training opportunities is available to all staff members, including whole school activities and CPD training courses via the ROSIS brochure.
- All staff will undergo e-safety training on a regular basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy.

4.3. Educating parents:

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Twilight courses and presentations will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1. Internet access:

- A record will be kept by the school of all pupils who have been granted internet access.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the head teacher.
- All school systems will be protected by up-to-date virus software.

- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Master users' passwords will be available to the head teacher for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the IT Technician for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from using any personal devices. This will be dealt with following the process outlined in section 7.4 of this policy.

Email:

- Staff will be given approved email accounts and are only able to use these accounts.
- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Staff members are aware that their email messages are not monitored.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.3. Social networking:

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the head teacher.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the head teacher prior to accessing the social media site.

5.4. Published content on the school website and images:

- The head teacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

5.5. Mobile devices and hand-held computers:

- The head teacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the IT Technician when using these on the school premises.

- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal mobile devices will not be used to take images or videos of pupils or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5.6. Network security:

- Network profiles for each pupil and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords will expire after 90 days to ensure maximum security for staff accounts.

5.7. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the IT Technician.
- The IT Technician will ensure that the filtering of websites and downloads is up-to-date and monitored.

6. Cyber bullying

6.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

6.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

6.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

6.7. The head teacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

7. Reporting misuse

7.1. Ferham Primary School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Aggreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

7.3. Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the head teacher, using CPOMS.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the head teacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

7.4. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the head teacher.
- The head teacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy, and may decide to take disciplinary action against the member of staff.

- The head teacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

7.5. Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and head teacher will be informed and the police contacted.

8. Monitoring and review

8.1. This policy will also be reviewed annually; any changes made to this policy will be communicated to all members of staff.

8.2. Members of staff are required to familiarise themselves with this policy as part of their induction programme

Ferham
Primary School

Staff, student and governors information systems code of conduct / Acceptable use policy

To ensure that all adults in our schools are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. We ask that all adults working in school consult the school's e-safety/Acceptable Use Policy for further information and clarification.

- The information systems (laptops, computers, web cameras etc) are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may not be used for private purposes, without specific permission from a member of the federation leadership team. This includes the use of personal networking sites (Facebook, Twitter etc) and sites used for personal profit e.g. Ebay.

- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

- I will not install any software or hardware to any school computer or laptop without permission.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- When using a personal device to access school emails or other school related websites (e.g Eazmag) I will ensure I follow a two-step authentication process. I will also ensure that access to such websites is only gained through a secure WIFI provider.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the school e-Safety coordinator or the designated safeguarding lead. This includes reporting any inappropriate websites, images or sounds which have made it through the schools firewall and filtering systems. I will also report any allegations or evidence of cyber-bullying to the safe guarding team.

- I will remember to conduct myself online as I would do in the 'real' world in my professional capacity.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create. I will help educate my pupils about the effects and consequences of cyber-bullying and teach them ways of avoiding and dealing with this.

- If at any time I have concerns/worries about the e-safety of myself or pupils within school I will consult with the safeguarding team.

- I understand that failure to follow the school Acceptable Use and e-safety Policy may result in disciplinary action being taken against me by the school, governing body or the local authority.

- School insurance cover provides for the standard risks but excludes theft when left inappropriately unattended. This means that at the end of the school day laptops should be **locked** away and when away from school premises they should **never be left unattended.**

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Social Networking Code of Conduct

The following are **not considered acceptable** at Ferham Primary School

- The use of the school's name, logo, or any other published material without written prior permission from the Head teacher. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school.

In addition to the above everyone must ensure that they:

- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.

- Use social networking sites responsibly and ensure that neither their personal/professional reputation, nor the school's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

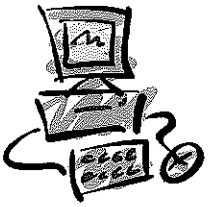
- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school

I have read and understand the information systems code of conduct/ acceptable use policy

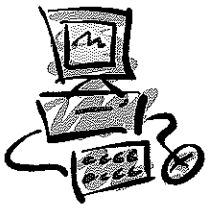
Name:_____.

Signed:_____**.Date:**_____.

Ferham
Primary School



E-Safety Rules



Our e-safety rules will be shared with our children and displayed in our classrooms

- Never give out personal information such as name, address, phone numbers, school name
- Only use a computer when an adult is nearby
- Tell an adult of you come across anything that makes you fell upset or uncomfortable
- Never send a picture of yourself to someone you don't know or haven't met
- Never arrange to meet someone that you have met on the internet.
- Never give your passwords to anyone
- Don't fill forms out online without asking an adult first
- Check with an adult before downloading anything as it may harm your computer