

Hutton Cranswick CP School



Together We Achieve

E-Safety Policy

Date Completed: March 2019

Review Date: March 2020

Hutton Cranswick C P School

E-Safety Policy

Statement of intent

At Hutton Cranswick CP 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 mitigate the risk of harm.

1. Legal framework

- 1.1. This policy has due regard to all relevant legislation including, but not limited to:
 - The General Data Protection Regulation
 - Freedom of Information Act 2000
- 1.2. This policy also has regard to the following statutory guidance:
 - DfE (2018) 'Keeping children safe in education'
 - National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- 1.3. This policy will be used in conjunction with the following school policies and procedures:
 - Behaviour Policy
 - Child Protection/Safeguarding Policy
 - Anti-Bullying Policy
 - Privacy Notices (Staff/Parents/Carers)
 - Records Management Policy
 - Acceptable Use Agreement
 - Data Protection Policy

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 the following:
 - 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. content 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 of the 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 computing subject leader, Mike Nevet, is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.
- 3.4. The headteacher is responsible for ensuring that the computing subject leader and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.
- 3.5. The computing subject leader 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 headteacher and computing subject leader will ensure there is a system in place to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.
- 3.7. The computing subject leader will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.
- 3.8. The headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
- 3.9. The computing subject leader will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.
- 3.10. The link governor will hold regular meetings with the computing subject leader 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.
- 3.11. The computing subject leader and link governor will evaluate and review this E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/pupils.
- 3.12. The headteacher will review and amend this policy with the e-safety officer, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- 3.13. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
- 3.14. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.
- 3.15. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the School Business Manger.

- 3.16. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.
- 3.17. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.
- 3.18. 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

Educating pupils:

- 4.1. 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.
- 4.2. 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.
- 4.3. Pupils will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.
- 4.4. Pupils are instructed to report any suspicious use of the internet and digital devices to their classroom teacher or appropriate adult.
- 4.5. 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.
- 4.6. The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

Educating staff:

- 4.1. E-safety training opportunities are available to all staff members, including whole school activities and CPD training courses.
- 4.2. All staff will undergo e-safety training on an annual 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.
- 4.3. All staff will undergo regular audits by the computing subject leader in order to identify areas of training need.
- 4.4. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- 4.5. All staff will be educated on which sites are deemed appropriate and inappropriate.
- 4.6. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- 4.7. Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.
- 4.8. The computing subject leader will act as the first point of contact for staff requiring e-safety advice.

Educating parents:

- 4.1. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- 4.2. Twilight courses and presentations will be run by the school for parents.

- 4.3. Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

Internet access:

- 5.1. All users will be provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.
- 5.2. Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- 5.3. 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.
- 5.4. 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.
- 5.5. The governing body will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- 5.6. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- 5.7. All school systems will be protected by up-to-date virus software.
- 5.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- 5.9. Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- 5.10. Personal use will only be monitored by the headteacher for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.
- 5.11. 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 the misuse by staff section of this policy.

Email:

- 5.12. Staff will be given approved email accounts.
- 5.13. The use of personal email accounts to send and receive personal data or information is prohibited.
- 5.14. No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- 5.15. Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- 5.16. Staff members are aware that their email messages are not monitored.
- 5.17. Chain letters, spam and all other emails from unknown sources will be deleted without opening.
- 5.18. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The computing subject leader will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

- 5.1. Access to social networking sites will be filtered as appropriate.

- 5.2. 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 headteacher.
- 5.3. Pupils are regularly educated on the implications of posting personal data online outside of the school.
- 5.4. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- 5.5. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- 5.6. Staff are not permitted to publish comments about the school which may affect its reputation.
- 5.7. Staff are permitted to use social media to post updates on good practice but are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

Published content on the school website:

- 5.8. The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.
- 5.9. 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.
- 5.10. 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.
- 5.11. Pupils are not permitted to take or publish photos of others without permission from the individual.
- 5.12. 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.

Mobile devices and hand-held computers:

- 5.13. Mobile devices are not permitted to be used during school hours by pupils.
- 5.14. The sending of inappropriate messages or images from mobile devices is prohibited.
- 5.15. Mobile devices will not be used to take images or videos of pupils or staff.
- 5.16. No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks. Primary Tec will inform staff members of this rule before they can use school-owned devices away from the premises.
- 5.17. All mobile devices and hand-held computers will be fitted with tracking software to ensure they can be retrieved if lost or stolen.
- 5.18. To protect, retrieve and erase personal data, all mobile devices and hand-held computers will be fitted with software to ensure they can be remotely accessed.
- 5.19. Primary Tec will review all mobile devices and hand-held computers on an annual basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.
- 5.20. The headteacher and the computing subject leader will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from the headteacher or the computing subject leader.
- 5.21. Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Network security:

- 5.22. 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.
- 5.23. Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- 5.24. Passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.
- 5.25. The Primary Tec will ensure all school-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.

Virus management:

- 5.26. Technical security features, such as virus software, are kept up-to-date and managed by the Primary Tec.
- 5.27. The computing subject leader will ensure that the filtering of websites and downloads is up-to-date and monitored.
- 5.28. Firewalls will be switched on at all times – Primary Tec will review these as per contract to ensure they are running correctly and to carry out any required updates.
- 5.29. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's contract with Primary Tec.
- 5.30. Staff members will report all malware and virus attacks to the computing subject leader and/or headteacher immediately.

E-safety committee:

- 5.31. The E-safety Policy will be monitored and evaluated by the computing subject leader, link governor and headteacher on an annual basis.

6. Cyber bullying

- 6.1. For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.
- 6.2. The school recognises that both staff and pupils may experience cyber bullying and is committed to responding appropriately to 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 utmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.
- 6.7. The headteacher 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. Hutton Cranswick C P School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, 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.

Misuse by pupils:

- 7.3. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher.
- 7.4. Parents/carers will be contacted for any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet.
- 7.5. 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.

Misuse by staff:

- 7.6. Any misuse of the internet by a member of staff should be immediately reported to the headteacher.
- 7.7. The headteacher will deal with such incidents in accordance with the Complaints Policy and may decide to take disciplinary action against the member of staff.
- 7.8. The headteacher 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.

Use of illegal material:

- 7.9. In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.
- 7.10. 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.
- 7.11. If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.
- 7.12. Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

8. Monitoring and review

- 8.1. The headteacher, computing subject leader and link governor will evaluate and review this E-safety Policy on an annual basis, taking into account the school's e-safety training, the latest developments in ICT and feedback from staff/pupils.
- 8.2. Any changes made to this policy will be communicated to all members of staff.
- 8.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.