Waverley Abbey's E-Safety Procedures

Introduction

At Waverley Abbey C of E Junior 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 procedure in line with the Acceptable Use Policy (AUP) 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.

The updated draft guidance contains additional information and clarification related to E-safety, including:

- A new section dedicated to online safety; it sets out how schools should ensure that appropriate filtering and monitoring systems are in place, and that such systems should be able to identify pupils accessing or trying to access, harmful or inappropriate material.
- Rewording from "should consider" to "should ensure" with regards to how schools will teach their pupils about safeguarding, including online.
- Clarifying that whilst it is important for schools to ensure that appropriate filters and monitoring systems are in place, "over blocking" should not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- Stating that 'the use of mobile technology' should be included in schools' child protection and safeguarding policies. Once published, this procedure and AUP will be updated to reflect any new requirements.

Effective technical security depends not only on technical measures, but also on appropriate policies, procedures and on good user education and training.

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- Pupils can only access data to which they have right of access.
- Logs are maintained of access by users and of their actions while users of the system.
- There is effective guidance and training for pupils.
- There are regular reviews and audits of the safety and security of school computer systems.

Technical Security

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within these procedures and the Acceptable Use Policy are implemented.

- There will be regular reviews and audits of the safety and security of school's technical systems
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to our on-site ICT Technicians.
- All pupils will have clearly defined access rights to school technical systems.

- Pupils will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details..
- Waverley Abbey's ICT Technicians regularly monitor the activity of users on the school technical systems and pupils are made aware of this in the Acceptable Use Policy.
- ICT Staff that manage the filtering systems have clear procedures for reporting issues.

A safe and secure username and password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Pupil Passwords

- All pupils will be provided with a username and password by our ICT Technicians who will keep an up to date record of users and their usernames.
- Y5 and Y6 will be required to change their password annually.
- Pupils will be taught the importance of password security
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Education, Training and Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education program. They will also be warned of the consequences of attempting to subvert the filtering system.

Parents are informed of the school's filtering policy through the Acceptable Use Policy.
Pupils will be made aware of the school's password policy:

- In lessons
- Through the Acceptable Use Policy

Internet Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

Use of the Internet

The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools to implement, which minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful.
These risks include 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. involving radicalisation

- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual’s consent or knowledge

Roles and Responsibilities

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.
The school has established a procedure for reporting incidents and inappropriate internet use, either by pupils or staff. The Headteacher will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and the ICT Department will keep a log of all incidents recorded.

The ICT Department is responsible for ensuring the day-to-day e-safety in our school and managing any issues that may arise. The ICT Department will regularly monitor the provision of e-safety in the school.

The Headteacher is responsible for ensuring that relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

Cyber bullying incidents will be reported in accordance with the school’s Cyber Bullying and Anti- Bullying Policies.

Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times. All staff are responsible for ensuring they are up-to-date with current e-safety issues and the AUP.

All staff and pupils will ensure they understand and adhere to our Acceptable Use Policy, which they must sign and return to the school office. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

E-safety control measures

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.

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 and in the home school agreement. Pupils are instructed to report any suspicious use of the internet and digital devices.

Internet Access

Internet access will be authorised once parents and pupils have returned the signed consent form as part of our Acceptable Use Policy. A record will be kept by the school office of all pupils who have been granted internet access.

Management systems are 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 particular websites.

Any requests by staff for websites to be added or removed from the filtering list will first be authorised by the Headteacher.

All school systems are protected by up-to-date virus software.

Email

Staff will be given approved email accounts and are only able to use these accounts for school purposes. Use of personal email to send and receive personal data or information is prohibited. Any sensitive personal data shall only be sent to staff internally with encryption. No data of a sensitive nature must be sent to any external email addresses. Chain letters, spam and all other emails from unknown sources should be deleted without opening.

Social Networking

Use of social media on behalf of the school will be conducted following the processes outlined in our Staff Code of Conduct. 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 the ICT coordinator and must be first authorised by the Headteacher.

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 Headteacher prior to accessing the social media site

By default, access to all social media is blocked by web-filtering.

The School website and published content including images

The Headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate. All contact details on the school website will be the phone, 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 unless a parent has agreed at the start of the pupils school career. Pupils are not permitted to take or publish photos of others without permission from the individual.

Staff are able to take images, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take images 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.

Mobile Devices and Handheld Computers

The Headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use. Mobile devices are not permitted to be used during school hours.

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 ICT Department when using these on the school premises.

The sending of inappropriate messages or images from mobile devices is prohibited. Mobile devices must 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.

Virus Management

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

Cyber Bullying

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

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

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 Policies.

Reporting Misuse

Misuse by pupils:
Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use. Any instances of misuse will be logged in accordance to our e-safety concern procedure.

Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will be suspended from using it and a record will be kept and parents informed.

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 e-safety coordinator. 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 Policy.

Misuse by staff:
Any misuse of the internet by a member of staff should be immediately reported to the Headteacher preferably in writing. The Headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.