Emanuel School

E-Safety Policy

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other school policies such as the Child Protection and Safeguarding Policy, the Behaviour Policy, the Anti-Bullying Policy, Pupils Acceptable Use Policy and other policies and procedures referred to below.

This policy applies to all members of the school community (including staff, pupils, parents and visitors) who have access to the school's ICT facilities both in and out of the School.

Roles and Responsibilities

The deputy head: pastoral is responsible for monitoring the effectiveness of this policy. Staff log any e-safety incidents to the e-safety log on Firefly which is monitored by the deputy head: pastoral. The deputy head: pastoral will then discuss with members of staff, the pastoral team, counsellors and at pastoral committee meetings.

The IT director is responsible for ensuring that the school's technical infrastructure is as secure as possible; that only registered users may access the school's networks and devices; that appropriate filtering is applied and updated on a regular basis and that use of the school's

ICT facilities is regularly monitored to ensure compliance with Pupil Acceptable Use Policy and Staff Code of Conduct.

The designated safeguarding lead is responsible for ensuring that all e-safety incidents are logged in the e-safety log on Firefly and following up on any child protection issues that may arise out of an e-safety incident. This will be in accordance with the school's Safeguarding and Child Protection Policy.

All staff are responsible for ensuring that they have an up to date awareness of this policy, that they adhere to the school's Code of Conduct and Information Security policies, that they report any suspected misuse to the deputy head: pastoral or designated safeguarding lead as appropriate and that they help pupils to understand the E-Safety policy and related policies.

Pupils must ensure they adhere to the Pupil Acceptable Use Policy. They should understand the importance of reporting to a member of staff any abuse, misuse or access to inappropriate materials. They should also understand the importance of adopting good e-safety practice when using technology outside school and realise that the school's Behaviour, Anti-Bullying and E-Safety policies will cover their actions outside school if related to their membership of the school.

Parents are asked to support the school in promoting good e-safety practice and to follow the guidelines in this policy.

Use of technology in school

All use of the school network, of personal devices in school and of devices owned by the school (whether on or off the school site) must comply with the Laptop and Mobile Device Policy. Failure to comply with the policy may result in disciplinary sanctions for pupils in accordance with the school's Behaviour Policy and for staff under the school's Disciplinary Procedure.

Personal devices should be switched off and kept out of sight during timetabled lessons unless the teacher has given express permission for them to be used; while moving between lessons; in the refectory, chapel, library, lower school playground or during assemblies. If a personal device is deemed by a member of staff to be causing a distraction around school, it is liable to confiscation until the end of the school day. Pupils may use their mobile phone before registration and after school. Pupils in the middle school and above may use their phones during break and lunchtime.

Wearable tech are devices that can be worn on the body, either as an accessory or as part of material used in clothing, and is able to connect to the internet, enabling data to be exchanged between a network and the device, for instance an apple watch or fitbit. If wearable tech is worn in lessons or in public areas around the school, then the 'do not disturb' or 'flight' mode should be activated.

Pupils must not have any device capable of mobile communication e.g. a mobile phone or wearable tech in either internal or public examinations as this will result in disqualification.

Technical infrastructure

The IT department reviews and audits the safety and security of the school's technical systems. This will periodically be supplemented by an external audit and review.

- Servers, wireless systems and cabling is securely located and physical access is restricted.

- All users are provided with a user name and password by the IT department. Users are responsible for the security of their user name and password.
- The school monitors, controls and filters internet access for all users. Websites containing illegal, pornographic, violent, abusive, terrorist or extremist material are blocked. Instant messaging and social networking sites, as well as gaming and other similar sites, will be blocked unless specifically authorised by the director of IT and deputy head: pastoral.
- Websites visited are recorded and monitored by the IT department. The designated safeguarding lead reviews sites flagged as potentially intolerant and monitors for patterns and issues of concern. Data transfer to and from the school's facilities will be subjected to virus scanning and filtering.
- The school would normally only access, monitor and control an individual user's data in response to specific circumstances which might imply possible misuse and following specific authorisation from either the headmaster or director of finance and administration.

Staff awareness

All new members of staff receive information on the school's E-Safety Policy and Code of Conduct as part of their induction.

Teaching staff receive information about e-safety issues at staff meetings as and when required and as part of their regular safeguarding training updates.

Pupil education and information

All new pupils receive a copy of the school's Pupil Acceptable Use Policy. They are encouraged to discuss its contents with a parent or teacher.

The school's Life Education programme incorporates e-safety information in the context of cyberbullying and also emphasises the need to build resilience in pupils.

Key e-safety messages are delivered in assemblies or form time. External speakers are also invited to speak to pupils, and sometimes parents, on e-safety topics.

Use of images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. social networking sites).

Pupils, staff and parents should refer to the Taking, Storing and Using Images of Children Policy for further information on how to safely use images of children.

Data Protection

The school has a Data Protection Policy which outlines how the school will comply with the General Data Protection Regulation and UK Data Protection Act. The school's Information Security Policy advises staff on how best to keep information secure. The school must ensure that appropriate security measures are taken to prevent unlawful or unauthorised processing of the personal data and against the accidental loss of personal data.

Staff must not remove personal data from the school's premises unless it is on a password protected computer or a memory device provided by the school, with the exception that the school's data management system may be accessed remotely from password protected devices and relevant personal data about pupils out of school on a visit may be carried by accompanying members of staff.

Social networking sites

Social networking applications include, but are not limited to: blogs; online discussion forums; collaborative spaces; media sharing services (e.g. youtube; and 'micro blogging' applications (e.g. twitter)).

Staff and pupils must not access social networking sites for personal use via school information systems, school networks or using school equipment. The school's filtering system is designed to block access to such sites as a matter of course.

If a member of staff considers that access to a social networking site would be appropriate for staff or a group of pupils for curricular or extra-curricular purposes, a proposal must be submitted to the IT director and deputy head: pastoral, and authorisation received in advance. The use of social networking sites within school will only be permitted in appropriately controlled situations.

Staff must not publish anything which could identify pupils, parents or guardians on any personal social media account, personal webpage or similar platform. This includes photos, videos, or other materials such as pupil work. Staff must not privately connect with or be "friends" with pupils on any social media or other interactive network. See also the Staff Code of Conduct.

Procedures for dealing with e-safety incidents involving pupils

If a pupil feels uncomfortable or worried by anything online or on a device, they should tell a member of staff or parent as soon as possible.

Any allegation, complaint, concern or suspicion that a pupil has been involved in any of the following should be reported immediately to the designated safeguarding lead and action will be taken in accordance with the school's Safeguarding and Child Protection Policy:

- Possession of, or access/attempted access to a website containing, images of child abuse;
- Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;
- Any incident by electronic means involving 'grooming' behaviour;
- Any other incident (which may include instances of cyber-bully or 'sexting') that suggests that a pupil or another child has suffered or is at risk of suffering serious harm.

Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft, unlicensed use of software or unlawful use of personal data should be reported to the deputy head: pastoral. Such concerns will be managed in accordance with the school's Behaviour Policy although referrals may be made to outside agencies as appropriate.

Any concern or allegation regarding 'sexting' should be reported to the deputy head: pastoral or the designated safeguarding lead. 'Sexting' may constitute abuse or a criminal offence and will be considered in accordance with the school's Safeguarding and Child Protection Policy and guidance published by the UK Council for Child Internet Safety: '*Sexting in schools and* *colleges: responding to incidents and safeguarding young people*'. Incidents involving 'sexting' will be recorded on the school's e-safety incident log.

Any allegation of cyber-bullying which is not referred to above should be reported to the deputy head: pastoral as soon as possible. Cyber-bullying incidents will be dealt with in accordance with the school's Anti-Bullying and Behaviour policies.

Any other misuse of the school's IT facilities not falling within one of the categories above should be referred to the deputy head: pastoral who will take action as appropriate in accordance with the school's Behaviour Policy.

Procedures for dealing with e-safety incidents involving staff

Any allegation, complaint, concern or suspicion that a member of staff has been involved in any of the following should be reported immediately to the designated safeguarding lead and the headmaster (or to the chair of governors if the headmaster is the subject of the concern):

- Possession of, or access/attempted access to websites containing images of child abuse;
- Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;
- Any incident by electronic means involving 'grooming' behaviour;
- Any other incident that suggests that a pupil or another child has suffered or is at risk of suffering serious harm from a member of staff.

Concerns or allegations regarding other technology related illegal activity such as fraud, copyright theft or unlawful use of personal data should be reported to the headmaster or the director of finance and administration immediately. Such concerns will be managed in accordance with the school's Whistleblowing Policy and disciplinary procedures and will be referred to the police as appropriate.

Any other misuse of the school's IT facilities not falling within one of the categories above should be referred to the director of finance and administration who will take action as appropriate in accordance with the school's disciplinary procedures.

Collecting and preserving evidence

If a member of staff suspects or is informed that there are indecent or obscene images of a pupil or another child on a device, the member of staff should not attempt to search for or print off such images as this may in itself constitute a criminal offence. The device should be confiscated, secured and handed directly to the designated safeguarding lead. The designated safeguarding lead and another member of SMT or a head of section will investigate further, using guidelines developed by CEOP (Child Exploitation and Online Protection centre) and the UK Council for Child Internet Safety.

For guidance on collecting and preserving electronic evidence in other instances, particularly where there has been an allegation of cyber-bullying, see Appendix 1 to this policy. The IT department can also be consulted to assist in establishing, capturing or preserving relevant data or other evidence.

Related documents

- Pupil Acceptable Use Policy
- Laptop and Mobile Device Policy

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy
- Information Security Policy
- Taking, Storing and Using Images of Children Policy

Appendix 1: The collection and preservation of evidence

If you suspect that there are indecent or obscene images of a pupil or another child on a device, you should not attempt to search for or print off such images as suggested in this appendix as this may in itself constitute a criminal offence. The device should instead be confiscated, secured and handed directly to the designated safeguarding lead. The following applies to situations which do not fall into this category.

Preserve the evidence

Advise pupils and staff to try to keep a record of the abuse/misuse, particularly the date and time, the content of the message(s), and where possible a sender's ID (e.g. username, email, mobile phone number, IP address) or the web address of the profile/content. For example, taking an accurate copy or recording of the whole webpage address will help the service provider to locate the relevant content. Keeping the evidence will help in any investigation by the service provider, but it can also be useful in showing what has happened to those who may need to know, including parents, teachers, pastoral staff and the police.

It is always useful to keep a written record, but it is better to save evidence on the device itself:

Mobile phones

Ensure the recipient keeps/saves any messages, whether voice, image or text. Unfortunately forwarding messages, e.g. to a teacher’s phone, can result in loss of information from the original message, such as the sender's phone number.

Instant messaging (IM)

Some services allow the user to record all conversations. The user could also copy and paste, and save and print these. Copied and pasted conversations can be edited so are less useful as evidence to the service provider or the police. Conversations recorded/archived by the IM service are better for evidence here. Conversations can also be printed out in hard copy or sections can be saved as a screen-grab.

Social networking and chatrooms

On social networking sites, video hosting sites, or other websites, keep the site link, print page or produce a screen-grab of the page and save it. To take a copy of what appears on the screen, press Control and Print Screen, and then paste this into a word-processing document.

Email

The recipient should print the email and forward the message on to the staff member investigating the incident. They should be encouraged to forward and save any subsequent messages. Preserving the whole message, not just the text, is more useful as this will contain 'headers' (information about the source of the message).

Threats

Use the ‘Report abuse’ button that usually is provided by most social networking services. Threatening phone messages should be preserved and depending on the nature and tone of the threats made, parents should consider contacting the police at an early opportunity in order to get the best advice at an early stage. The school should also be informed at an early opportunity in order that on a need to know basis, staff can be aware and put in place procedures to monitor and support the pupil.

Appendix 11: E-Safety Incident Report Form

The form is available on Firefly: https://emanuel.fireflycloud.net/it-department/e-safety-incident-report-form

Name of staff reporting	
Date and time of incident	
Where did the incident occur?	
Who was involved in the incident? **(Name of student / staff / other)**	
Description of incidents? **(including IP addresses, usernames, devices and programmes used etc.)**	
Action taken	Incident reported to headmaster
	Incident reported to Police
	Incident report to IT
	Disciplinary action to be taken
	E-Safety Policy to be reviewed
	Advice sought from social and safeguarding services
	Other
Outcome of investigation	