Emanuel School

E-Safety Policy

Introduction

Technology is integral to the lives of children and young people in today's society, both within and outwith school. The internet, social media and other digital 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 technologies can put young people at risk. 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 Safeguarding and Child Protection Policy, the Behaviour Policy, the Anti-Bullying Policy, Pupil Acceptable Use Policy, Laptop and Mobile Device Policyand other policies and procedures referred to below.

At the start of each academic year, the Pupil Acceptable Use Policy is sent to the parents of all new pupils, and reviewed by form tutors with their tutees. This policy outlines expected behaviour when using electronic devices and online.

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 should report any e-safety incidents or concerns to the relevant head of section and deputy head: pastoral who will investigate and retain a record as appropriate. The deputy head: pastoral will then discuss with staff, the pastoral team, counsellors and at pastoral committee meetings. As the designated safeguarding lead, the deputy head: pastoral is also responsible for 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.

The head of IT and compliance 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.

All staff (including staff who are absent from the school for a period of time) 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 at all times, that they report any suspected misuse to the deputy head: pastoral 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.

Mobile phones should be switched off and kept out of sight during the school day unless a teacher has given express permission for them to be used. Pupils in the lower and middle schools must turn off their phones and lock them in their lockers each morning and collect them only at the end of the day. They must not be accessed at break or lunch without permission.

Pupils in the sixth form may use their mobile phones in the sixth form centre only during break and lunch.

Mobile phones should not be used in any manner or place that is disruptive to the normal routine of the school. Pupils who do not abide by these rules may receive a behavioural sanction and may have their phone confiscated.

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 may 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 username and password by the IT department. Users are responsible for the security of their username 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 head of IT & compliance 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 deputy head: pastoral or bursar.

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, and undertake online training on relevant topics.

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 and their parents receive a copy of the school's Pupil Acceptable Use Policy at the start of the school year.

The school's Life Education programme and Computing classes teach pupils about online safety, including developing knowledge and behaviours to help pupils navigate the online world safely and confidently and incorporates e-safety information in the context of cyberbullying and also emphasises the need to build resilience in pupils. This includes navigating the internet and managing information, how to stay safe online and covering elements of online activity that can adversely affect a pupil's wellbeing. Key e-safety messages are also delivered in assemblies or form time. External speakers are also invited to speak to pupils, and sometimes parents, on e-safety topics.

Pupils in the middle school will complete an AI-powered adaptive learning course from Digital Awareness UK throughout the school year. This will be delivered during life education and form assemblies. The cloud base platform delivers an interactive learning experience through a range of informative and engaging videos, quizzes and learning resources. They will complete ten online courses including balance & screens, sexting and the law, scams, posture wellness, sleep & screens, trash talk & in-game abuse, hacking, digital eye strain, online hate speech and algorithms.

Examples from the school's curriculum include:

Lower School	
Y6	• Well-being and social media. What are the positives and negatives. Other ways to communicate and have fun. Signposting. • Newswise – what to believe and what to question • Internet content and contact (Be SMART online) • Risks of network devices including Firewalls, Anti-virus, Hacking, Strong passwords and Data Protection
Y7	• Cyberbullying: • Digital resilience: • Risks of network devices including Firewalls, Anti-virus, Hacking, Strong password and Data Protection
Y8	• Well being and social media: Using social media responsibly and the importance of offline activities: • Online Stress: Online friends v real and FOMO • Sexting • Review of the risks of network devices including Firewalls, Anti-virus, Hacking, Strong password and Data Protection
Middle School	
Y9	• Online stress & FOMO • Bullying & cyberbullying • To stream or not to stream (the risks of livestreaming) • Review of the risks of network devices including Firewalls, Anti-virus, Hacking, Strong password and Data Protection
Y10	• The risks of online grooming and how to establish digital resilience, as well as making better choices when interacting online. - Breck Foundation Revenge porn & the law on sharing nude pictures
Y11	• The risks associated with gambling & gaming • Identifying unhealthy relationships • Managing unwanted attention Pornography – Online pressures & perceived norms

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's Data Protection Policy outlines how the school will comply with data protection legislation. The Information Security Policy advises staff on how best to keep information secure and staff should ensure they take appropriate security measures to prevent unlawful or unauthorised processing of the personal data and against the accidental loss of personal data.

Social media and networking sites

Social media and networking sites allow anyone to create a public profile and interact with other users of the application or site.

Staff and pupils must not access social media or 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 deputy head: pastoral and head of IT and compliance, and authorisation received in advance. The use of social networking sites within school will only be permitted in appropriately controlled situations.

Outside of the school's official social media accounts, 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 and Safeguarding and Child Protection Policy.

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. Pupils can also use the button on Firefly to report any pastoral (including online) concerns.

Any allegation, complaint, concern or suspicion that a pupil has been involved in any of the following should be reported immediately to the deputy head: pastoral (as 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. '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 bursar 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 bursar 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
- Remote Learning 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.

Social media and 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 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

Most social media and networking sites provide a 'reporting' function which should be used when appropriate. 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.