Godolphin&Latymer

# E-Safety Policy

Reviewer: AP June 2018

Next review date June 2019

**This Policy is available to parents on the school website or as a paper copy on request to the School Office.**

## 1. Introduction

1.1. 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.

1.2. 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.

1.3. 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 (Child Protection) Policy, the Behaviour Policy, the Anti-Bullying Policy, Acceptable Use of ICT policies and other policies and procedures referred to below.

1.4. 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.

## 2. Roles and Responsibilities

2.1. ***The Senior Deputy Head (Pastoral)*** is responsible for approving this policy and for monitoring its effectiveness. This is carried out via discussions with members of staff, the pastoral team, counsellors and at Safeguarding Committee meetings.

2.2. ***The IT Network Manager*** 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 Acceptable Use Policies.

2.3. ***The Designated Safeguarding Lead*** is responsible for maintaining the e-safety incident log 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 (Child Protection) Policy.

2.4. ***All staff*** are responsible for ensuring that they have an up to date awareness of this policy, that they adhere to the School's Acceptable Use of ICT and Information Security policies, that they report any suspected misuse to the Senior Deputy Head (Pastoral) or Designated Safeguarding Lead as appropriate and that they help pupils to understand the E-Safety policy and related policies.

2.5. ***Pupils*** must ensure they adhere to the Code of Conduct for Pupil's Use of ICT. 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.

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

## 3. Use of Technology in School

3.1. ***Acceptable Use Agreements***: 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 Acceptable Use of ICT for Staff Policy or the Code of Conduct for Pupils' Use of ICT as applicable. Any devices used during the school day must access the internet via the School's wireless network and 'hot-spotting' via a mobile phone is strictly prohibited. Failure to comply with the relevant Acceptable Use agreement may result in disciplinary sanctions for pupils in accordance with the School's Behaviour Policy and for staff under the School's Disciplinary Procedure.

3.2. ***Devices owned by the School*** may be assigned to staff or pupils for short-term or longer-term use. Devices assigned for short-term use (for example in a particular lesson, for an exam or a school visit) must be signed in and out by the member of staff responsible. Devices assigned for longer-term use are subject to a separate agreement which must signed by the member of staff or pupil at the time the devices is issued.

3.3. ***Personal Devices*** may not be used by pupils in the Lower and Middle School during the School day without the express permission of a member of staff. The Sixth Form have permission to use personal devices with certain restrictions (see the School's Behaviour Policy). Pupils must not have any device capable of mobile communication in examinations as this will result in disqualification. 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.

3.4. ***Wearable Tech*** includes electronics 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. 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.

## 4. Technical Infrastructure

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

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

4.3. 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.

4.4. 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 IT Network Manager and Senior Teacher responsible for Teaching and Learning. Controls for Sixth Form users may, with parental permission, be less stringent than for pupils in the Lower and Middle School.

4.5. Websites visited are recorded and monitored by the ICT 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.

4.6. 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 Head Mistress or Bursar.

## 5. Staff Awareness

5.1. All new members of staff receive information on the School's E-Safety and Acceptable Use policies as part of their induction.

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

5.3. The School has appointed a Pastoral Enrichment Assistant who will help ensure that staff awareness of, and training in, e-safety is current and appropriate.

## 6. Pupil Education and Information

6.1. All new pupils receive a copy of the School's Code of Conduct for Pupils' Use of ICT. They are encouraged to discuss its contents with a parent or teacher and then to sign to confirm that they will adhere to its terms.

6.2. The School's PSHE programme incorporates e-safety information in the context of cyber-bullying and also emphasises the need to build resilience in pupils.

6.3. Key e-safety messages are delivered in assemblies or form time. External speakers will also be invited to speak to pupils, and sometimes parents, on e-safety topics. Peer education works particularly well in the context of e-safety and Digital Ambassadors from a range of year groups assist with this peer education.

## 7. Use of Images

7.1. 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).

7.2. Staff are allowed to take and use images to support educational aims but must follow the School's policies concerning the sharing, distribution and publication of those images (e.g. the Taking, Storing and Using Images of Children Policy). Such images should be taken using school equipment where practicable. If images are taken on a personal device, the images should be downloaded to the school intranet at the earliest opportunity and deleted both from the personal device and from all related cloud back-ups.

7.3. Parents agree, via the School's Terms and Conditions, to the School using photographs of their daughter for promotional, media or educational purposes. If parents do not want their daughter's photograph or image to be used for these purposes they must make sure their daughter knows this and must write immediately to the Bursar requesting an acknowledgement of their letter.

7.4. Parents wishing to take photographs or record images of their daughter during School events such as dramatic or musical performances or at sporting fixtures may do so provided that this is for personal viewing by the Pupil and her immediate family only.

7.5. Pupils must not take, use, share, publish or distribute images of others without their permission.

## 8. Data Protection

8.1. The School has a Data Protection Policy which includes electronic data and an Information Security Policy which advises staff on how best to keep information secure.

8.2. 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.

8.3. Staff must not remove Personal Data from the School's premises unless it is stored in an encrypted form 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.

## 9. Social Networking Sites

9.1. 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)).

9.2. Staff and students 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.

9.3. 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 Network Manager and Senior Teacher responsible for Teaching and Learning and authorisation received in advance. The use of social networking sites within school will only be permitted in appropriately controlled situations.

9.4. 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 Acceptable Use of ICT for Staff policy.

## 10. Procedures for dealing with e-safety incidents involving pupils

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

10.2. 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 (Child Protection) Policy:

10.2.1. Possession of, or access/attempted access to a website containing, images of child abuse;

10.2.2. Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;

10.2.3. Any incident by electronic means involving 'grooming' behaviour;

10.2.4. 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.

10.3. 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 Senior 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.

10.4. Any concern or allegation regarding 'sexting' (also known as 'youth produced sexual imagery') should be reported to the Senior 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 (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 (see paragraph 2.4 above).

10.5. Any allegation of cyber-bullying which does not fall within 10.2.4 above should be reported to the Senior 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.

10.6. Any other misuse of the School's ICT facilities not falling within one of the categories above should be referred to the Senior Deputy Head (Pastoral) who will take action as appropriate in accordance with the School's Behaviour policy.

## 11. Procedures for dealing with e-safety incidents involving staff

11.1. 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 Head Mistress (or to the Chair of Governors if the Head Mistress is the subject of the concern) and action will be taken in accordance with the School's Safeguarding (Child Protection) Policy, Appendix 4:

11.1.1. Possession of, or access/attempted access to a website containing, images of child abuse;

11.1.2. Possession of, or access/attempted access to a website containing, illegal (e.g. obscene or criminally racist) or terrorist or extremist material;

11.1.3. Any incident by electronic means involving 'grooming' behaviour;

11.1.4. 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.

11.2. 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 Head Mistress 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.

11.3. Any other misuse of the School's ICT 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.

## 12. Collecting and preserving evidence

12.1. 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 SLT 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.

12.2. 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 Network Manager can also be consulted to assist in establishing, capturing or preserving relevant data or other evidence.

**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.

**How to do this**
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**
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.

**Chatrooms**
Print the page or produce a screen-grab of the page. To copy what is on the screen, press Control and Print Screen, then paste 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. Pupils and parents can use the CEOP panic button to report threatening or abusive contact made online. 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.