Godolphin & Latymer

Online Safety Policy

Reviewer: AP/AT October 2022
Education Committee: November 2022

Next review by: December 2023

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. The issues encompassed by the term 'online safety' are considerable and varied but can broadly be categorised into four areas of potential risk:

- ***Conduct***: children being put at risk because of their own behaviour; for example, by sharing too much information or explicit images;
- ***Content***: being exposed to illegal, inappropriate, unreliable or harmful material; for example pornography, racist or radical and extremist views;
- ***Contact***: being subjected to harmful online interaction with other users; for example children can be contacted by bullies or people who groom or seek to abuse them; and/or
- ***Commercial exploitation***: being unaware of hidden costs and advertising in apps, games and websites; for example inadvertently spending money within an app or game.

1.3. Many of these risks reflect situations in the off-line world and it is essential that this Online 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. It also applies to behaviour related to online safety, such as cyber-bullying, which may take place outside the school but which is linked to membership of the school. The school will address such behaviour in accordance with this policy and the Behaviour Policy.

2. Roles and Responsibilities

2.1. ***The Designated Safeguarding Lead*** has overall responsibility for online safety within the school and is responsible for the content and delivery of online safety education for pupils, staff and parents and ensuring that this is kept up to date. She is also responsible for maintaining the online safety incident log and monitoring it for emerging patterns or trends. She is responsible for following up on any child protection issues that may arise out of an online safety incident in accordance with the school's Safeguarding (Child Protection) Policy.

2.2. ***The Senior Deputy Head (Pastoral)*** is responsible for ensuring that online safety education is embedded in the PSHE and RSE curriculum to enable all pupils to develop an understanding of the risks as appropriate to their age and stage of development. She is responsible for approving this policy and for monitoring its effectiveness, including via

review of the online safety incident log in conjunction with the Designated Safeguarding Lead.

2.3. ***The IT Management Team*** (the Director of Digital Strategy and IT and the IT Network Manager) are 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.

2.4. ***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 Online Safety policy and related policies.

2.5. ***Pupils*** must engage with opportunities for learning about online safety and take responsibility for keeping themselves and others safe online both within and outside school. They must ensure they adhere to the Code of Conduct for Pupil's Use of ICT and understand the importance of reporting to a member of staff any abuse, misuse or access to inappropriate materials.

2.6. ***Parents*** are asked to support the school in promoting good online safety practice and to follow the guidelines in this policy.

3. Reducing Online Risks

3.1. The online world is constantly evolving with new apps, devices, websites and material emerging all the time. The school will:

- Ensure that appropriate filtering and monitoring is in place and take steps to ensure that users cannot access inappropriate material;
- Consider the educational benefit of emerging technologies before allowing their use in school; and
- Ensure, through online safety education and the school's policies and procedures, that pupils, staff and parents understand the school's expectations regarding safe and acceptable online behaviour both within and outside school.

4. Pupil Education and Information

4.1. 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 confirm that they will adhere to its terms.

4.2. The school's PSHE programme incorporates online safety information in the context of cyber-bullying and the sharing of inappropriate images.

4.3. Key online safety messages are delivered in assemblies or form time. External speakers may also be invited to speak to pupils, and sometimes parents, on online safety topics. Peer education works particularly well in the context of online safety and older students may be paired with younger form groups to deliver online safety sessions.

4.4. A summary of the Digital Wellbeing Scheme of Work is included in the Digital Safety Booklet with a more detailed version available to staff.

5. Staff Awareness

5.1. All new members of staff receive training on the school's Online Safety and Acceptable Use policies as part of their safeguarding induction. They are also given a copy of the Digital Safety Booklet.

5.2. All staff receive information about online safety issues at staff meetings as and when required and as part of their regular safeguarding training updates. The Digital Safety Booklet is updated every year and is sent out to all staff as a link, or via the minutes of staff meetings.

6. Engagement with Parents

6.1. The Digital Safety Booklet is updated every year and sent out annually at the start of the academic year usually via email.

7. Use of Technology in School

7.1. ***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.

7.2. ***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.

7.3. ***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.

7.4. ***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 must be activated.

8. Technical Infrastructure

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

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

8.3. 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. All users are automatically enrolled into MFA (Multi Factor Authentication)

8.4. 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 Management Team 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.

8.5. 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.

8.6. 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 or Bursar.

8.7. Personal data is collected, processed, stored and transferred in accordance with data protection legislation and the school's policies (see the Data Protection Policy for more information).

9. Social Media

9.1. Social media applications include, but are not limited to: blogs; wikis; social networking sites; online discussion forums; collaborative spaces; online gaming; apps; video/photo sharing services (e.g. Instagram/Youtube); chatrooms; instant messenger; and 'micro blogging' applications (e.g. Twitter)).

9.2. 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. Staff and students should not access social networking sites for personal use during school hours.

9.3. The safe and responsible use of social media is discussed with all new staff as part of their induction and is revisited with all staff during safeguarding update training. Safe and professional behaviour is outlined for all staff in the Acceptable Use of ICT for Staff Policy and the Staff Code of Conduct.

9.4. Safe and appropriate use of social media is taught to pupils as part of online safety education, via age-appropriate resources.

10. Procedures for dealing with online 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-bullying or sharing of inappropriate images or peer on peer abuse) that suggests that a pupil or another child has suffered or is at risk of suffering serious harm.

10.3. Any concern or allegation regarding the sharing of nudes or semi-nude images (also known as 'sexting' or youth produced sexual imagery) must be reported to the Designated Safeguarding Lead immediately. Staff must never view, copy, print, share, store or save the imagery themselves, or ask a child to share or download it, as this is illegal (if the image is viewed by accident this must be reported immediately to the DSL). Staff should not investigate the incident themselves or delete, or ask the child to delete, the image. The child should not be blamed or shamed but should be told that the incident will need to be reported to the DSL and that they will receive support and help. Action will be taken in accordance with this safeguarding policy, taking into account guidance published by the UK Council for Child Internet Safety: '*Sharing nudes and semi-nudes: advice for education settings working with children and young people*' which covers the creation and sharing of sexual imagery of those under 18 with others who are also under 18. Incidents involving 'sharing of nudes or semi-nudes will also be recorded by the DSL or Deputy DSL on the School's online safety incident log

10.4. 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 Management Team can also be consulted to assist in establishing, capturing or preserving relevant data or other evidence.

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 unless there is a risk of serious harm to a child and/or the incident constitutes peer on peer abuse, in which case it will also be dealt with under the School's Safeguarding (Child Protection) Policy.

10.6. 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.

10.7. Where there is suspicion that illegal activity has taken place, the school will contact the police using 101, or 999 if there is immediate danger or risk of harm.

10.8. 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 online 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 (or to the Chair of Governors if the Head is the subject of the concern) and action will be taken in accordance with the school's Safeguarding (Child Protection) Policy, Appendix 6:

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 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. Monitoring and Review

12.1. This policy will be reviewed at least annually and in response to any new guidance or legislation or significant developments in technology or in the event of a serious online safety incident.

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.