Godolphin & Latymer

Redcliffe Gardens School

Online Safety Policy

Reviewed: SG/PA October 2021
Prep School Committee: November 2021

Next review by: December 2022

This policy applies to the whole school including the EYFS.

1. Introduction

1.1. 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.

1.2. This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, governors, visitors) who have access to and are users of school ICT systems, both in and out of the school.

1.3. This policy should be read alongside other policies including those for Computing, Data Protection, Safeguarding (Child Protection), and Acceptable Use of ICT for Staff. This Online Safety policy has been agreed by senior leadership and approved by Governors. The policy and its implementation will be reviewed annually; senior leadership and the Online Safety and Computing coordinator will regularly monitor compliance and review the policy in light of any significant new developments in the use of the technologies, data protection, new threats to online safety or incidents that have taken place.

2. Education – Pupils

2.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build resilience.

2.2. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum, which should be broad, relevant and provide progression, with opportunities for creative activities, will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing and PSCHEE lessons, covering both school and home safe use
- Key online safety messages will be reinforced during assemblies
- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year
- Pupils will be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the Code of Conduct for Pupils' Use of ICT and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use
- If internet research is set for homework, specific sites will be suggested which have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research
- The School will supervise all access to internet resources (where reasonable) and pupils will not be allowed to use devices if there is not a supervisor present
    - At *Key Stage 1* all pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
    - At *Key Stage 2* all pupils will be supervised when using the internet. Pupils will use age-appropriate search engines and online tools; and online activities will be teacher-directed where necessary.
    - During remote learning all pupils will be supervised when using the internet by parents or guardians.

- The School subscribes to Britannica School and Britannica Images; all teachers, parents and pupils are encouraged to use the site as their first source of information when completing research or searching for images
- The School recommends the use of safe web searching websites
    - KidzSearch - https://www.kidzsearch.com/
    - Safe Search - https://www.safesearchkids.com/
    - YouTube kids - https://youtube.com/kids

3. Education – Parents / Carers

3.1. Parents and carers play an essential role in the education of their children and in the monitoring of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

3.2. The school will therefore seek to provide information and awareness to parents and carers through:

- Online Safety presentations
- List of suggested websites and apps posted on school website
- Provision of the Code of Conduct for Pupil use of ICT (Appendix 1)
- A Privacy Notice that describes how the School holds and uses their own and their child's personal data.

3.3. Parents will be responsible for monitoring their children's use of the internet whilst online at home and during remote learning sessions. They are provided with a copy of the Code of Conduct for Pupil Use of ICT.

4. Education & Training – Staff / Volunteers

4.1. It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy, and the Acceptable Use of ICT for Staff (in the Employment Handbook).
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings or on INSET days.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff will receive regular training and updates on the protection of personal information.
- Staff are provided with access to relevant guidance and training to enable remote learning as required.

5. Technical – Equipment, filtering and monitoring

5.1. 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 this policy are implemented.

5.2. It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

5.3. Technical measures include the following:

- There will be regular reviews and audits of the safety and security of school technical systems by the Godolphin & Latymer IT Team.
- All users will have clearly defined access rights to school technical systems and devices.
    - Staff will be provided with a username and secure password by the Godolphin & Latymer IT Team who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
    - Pupils will have logons.
- Internet access is filtered for all users.
- There is a clear process in place to deal with requests for filtering changes.
    - Staff may request that websites be removed from the blacklist by providing Godolphin & Latymer IT Team with the website.
    - Godolphin & Latymer IT Team will verify the website is safe before allowing access.
    - Godolphin & Latymer IT Team will keep a record of requested websites for administration to review.

- The internet filtering settings ensure that children are safe from terrorist and extremist material when accessing the internet.
- The School uses Smoothwall software to monitor internet use on pupil laptops, iPads and staff computers located in classrooms (where children may have access to them)
- Reporting Incidents (Staff):
    - All staff must report any actual or potential technical incidents or security breaches to the Head or the Designated Safeguarding Lead, in the first instance that they occur or that the member of staff becomes aware of them. Technical incidents and security breaches will also be reported to IT Management at G&L.
    - If a breach involves personal data it must also be reported to the Bursar/Assistant Bursar (Compliance).
    - Staff must isolate the device involved in the incident and not make any changes to the device (i.e. leave the iPad exactly as it is, do not close the webpage or turn off the computer)
    - The DSL will keep a log of all instances on the Safeguarding system, Safeguard.
    - The DSL & SLT will investigate and decide on an appropriate course of action in each instance.
- The school employs appropriate security measures to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Guest Access: The provision of access to guests will be addressed in the following way
    - Trainee and Supply Teachers- the Godolphin & Latymer IT Team create a unique login for teachers which are deactivated at their end of time with Redcliffe Gardens School.
    - Other guests will be provided with the WIFI password, should they require it, but not granted access to the school network.
- The ability to install programs is restricted to protect the school computers and prevent downloading of unsuitable content. Staff/pupils who wish to download programs must seek permission from Godolphin & Latymer's IT Team who will ensure the content is suitable and safe.
- Staff should use the school's secure drives and or Sharepoint for the storage of all data..
- Staff must use encrypted data USB if they need to transfer files that contain personal information about pupils or other staff.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

6. Use of Digital and Video Images

6.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes except with the express written permission of the Head.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupils work can only be published with the permission of the pupil and parents or carers.
- The Head will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Parents/Carers will be asked to sign a Use of Digital/Video Images consent form.
- Teachers should not live-stream lessons from their homes, nor engage in any video-calling unless in exceptional circumstances, with the parent(s) and the Head Teacher's permission.

7. Mobile Technology, Communications and Email

7.1. A wide range of rapidly developing communications technologies has the potential to enhance learning and teaching. The School provides staff and pupils with access to iPads and laptop computers for this purpose. The school will adhere to the following guidelines regarding mobile technology and pupil access:

- The school Code of Conduct for Use of ICT for staff and pupils, the latter of which is sent to parents, will give consideration to the use of mobile technology. The school allows staff to use personal and school owned devices to access the Internet. The

network may be accessed using school owned devices whilst at school, or via the individual's VPN credentials.

- Visitors to the school may be granted access to the Internet at the discretion of the staff member hosting the visitor, but not the network.
- Personal mobile devices for pupils are not permitted to be used in school. Any devices brought to school will be confiscated by the teacher/head and returned directly to the parent/carer at the end of the school day.

7.2. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Head, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Any contact between pupils and teachers should only be through a platform specified by the school and not through personalised accounts open to public viewing, comments or sharing.
- 'Live' lesson recording for use during remote learning should be made in a safe, neutral setting and conducted in a professional manner, including appropriate attire.

8. Data Protection

8.1. The School will ensure that we maintain confidentiality of records about staff and children, with access only available to those who have a right or a professional need to see them. Parents or carers must be given access to records about their child, provided that no relevant exemptions apply to their disclosure under the Data Protection Act and described in the Privacy Notice.

8.2. All personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations. Please refer to the school's Privacy Notice for Parents and Pupils or Privacy Notice for Staff.

8.3. When using technology, pupils and staff will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Delete personal data in line with the Data Retention Policy.

9. Responding to Incidents of Misuse

9.1. It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

9.2. **In the event of suspicion, all steps in this procedure should be followed:**

- **Report the suspicion** to the Designated Safeguarding Team or the Head. The report should never be investigated alone; this is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- Before any investigation into the misuse occurs, contact IT Lab to inform them of the intended investigation and the computer with which the investigation will be carried out on. They will then be able to monitor and record the sites and content visited (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may scanned into Safeguard **(except in the case of images of child sexual abuse – see below)**
- Once this has been completed and fully investigated the group will judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism

- other criminal conduct, activity or materials

- **Staff must always remember to isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

9.3. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

10. Cyber-bullying

10.1. Pupils will not be given access to social media whilst at school and will not have access to personal mobile devices. Lessons will be taught on how pupils can keep themselves safe, as well as not become perpetrators of, cyber-bullying. Pupils will discuss the Pupil Code of Conduct (See Appendix 1) The school will investigate all incidents of cyber-bullying that occur involving the pupils. For more information on the school's policy towards incidents of cyber-bullying, see the Anti-Bullying Policy.

Appendix 1:

Code of Conduct for Pupils' Use of ICT

Introduction

ICT, including the internet, email, mobile technologies and online resources, has become an important part of the learning experience. The School expects each pupil to be safe and responsible when using ICT and it is essential that the rules set out below are followed at all times for the protection of all pupils.
We therefore ask each pupil to read the following Code of Conduct for the Use of ICT, to discuss or raise questions about its contents with his parent, guardian or teacher as appropriate, and then to sign to indicate that he will be bound by its terms.

Code of Conduct for the Use of ICT

1. Use of School ICT Facilities

- I will only use the School's ICT facilities, including the internet, email, digital video and mobile technologies, for School purposes and in accordance with School policies.
- I will not attempt to circumvent systems and programmes that the School has put into place for my protection, such as filtering of websites on the School network and restriction of app downloads.
- I will only log onto the School Network or other School systems or resources with my own user name and password.
- I will not share my passwords with anyone else and I understand that the School will never send me an email requesting my password.
- I will not attempt to bypass the School's internet filtering system.

2. Use of Personally owned Devices

- I will not use a personally owned device such as a phone, tablet or laptop in School during the School day without the express permission of a teacher
- I will not connect a personally owned device to any of the School's projection facilities.
- If I am given permission to use a personally owned device during the School day, then that use is entirely at my own risk and it is up to me to ensure that the device is not damaged, lost or stolen.
- When in School or when completing school work at home I will only use a personally owned device in accordance with the rules set out in this agreement and the School's Behaviour and Anti-Bullying policies.
- If I have wearable technology in lessons or in public areas around the School, I will activate the 'do not disturb' or 'flight' mode.
- I understand that any personally owned device I use in School during the school day must access the internet via the school wireless network and that 'hot-spotting' via a mobile phone is strictly prohibited.

3. Responsible Behaviour

- I will make sure that all electronic communications with pupils, teachers or others are responsible, sensible and appropriate.
- I understand that I should never say anything in writing, electronic or otherwise, that I would not be prepared to say to someone's face.

- I will ensure that my online activity, both in school and outside school, will not cause staff, pupils or others distress or bring the School into disrepute.
- If I participate in any video conferencing with other pupils or staff. I will ensure that I am dressed appropriately and in a suitable location.
- I will only open a Google Meet when instructed to do so by a teacher using the code provided and will not invite anyone into a Google Meet without permission from a teacher.
- I will not deliberately browse, download, upload or forward material that could be considered hurtful, offensive or illegal. If I accidentally come across any such material I will not share or print it and will instead report it immediately to a member of staff.
- I am aware that I must ask permission before I take images or recordings of other pupils or staff and I must never distribute these by email, text, on the internet or via any social networking site without the express permission of all individuals involved.
- I will not give out any of my personal information online (such as name, phone number or address) nor that of other people.
- I understand that any information or images online are permanently accessible and may be seen by a school.
- I understand that I cannot be sure about the identity of a person I have only met online and I will not arrange to meet someone that I have only met online without a parent or guardian present.
- I will respect copyright and understand that submitting work that is not my own, without proper acknowledgment is not allowed.
- If anything makes me uncomfortable or worried, I know that I can share this with a teacher or parent/guardian.

4. Use of School iPads

- I will use the iPad for educational purposes only.
- I will use the iPad only for activities directly related to the lesson with the teacher's permission and I understand that the teacher may be able to view my iPad screen at any time during the lesson.
- I will place the iPad on the desk with the cover closed when not in use or when requested to stop using it by the teacher.
- I understand that taking or use of photos/video/recording on the iPad is not allowed without the subject's personal permission as well as the teacher's permission.
- I will not record lessons on the iPad without the teacher's permission.
- Within lessons, I will not communicate electronically with other pupils without permission from the teacher.
- If a member of staff asks to see my iPad's content or applications, I will show them immediately.

5. Monitoring and Sanctions

- I understand that my use of any of the School's ICT facilities, including the internet, email, digital video and mobile technologies, may be monitored and logged and may be made available to my teachers.
- I understand that these rules are designed to keep me safe and that any breach will be dealt with in accordance with the School's Behaviour Policy. Incidents involving breaches of this code of conduct will be judged on a case by case basis.