

CANBURY SCHOOL

# E-Safety Policy

**Introduction**

Online Safety Coordinator and Designated Safeguarding Lead: Mrs P Rich

Deputy Designated Safeguarding Lead: Ms L Clancy

IT Network Consultant: Mr S Harrison, Footprint Limited

It is the duty of Canbury School to ensure that every student in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

* Websites;
* Email;
* Instant messaging apps;
* Blogs;
* Social networking sites;
* Chat rooms;
* Music / video downloads;
* Games and gaming sites;
* Text messaging and picture messaging;
* Video calls;
* Podcasting;
* Online communities via games consoles; and
* Mobile internet devices such as smartphones and tablets.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and students), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

* Child Safeguarding Policy and Procedures;
* Student Behaviour, Sanctions and Rewards;
* Anti-Bullying;
* Social Media;
* Data Protection (for students and parents and for staff);
* Mobile Phone/Devices Policy

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Canbury School, we understand the responsibility to educate our students on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy and the Acceptable Use Policy and the Mobile Phones/Devices Policy (for all staff, visitors and students) cover all computing devices provided by the school (desktops, laptops, Chromebooks, cameras, iPads etc.); as well as all devices owned by students and staff brought onto school premises (personal laptops, tablets, smartphones, etc.).

#### Roles and responsibilities

The Online Safety Coordinator and the School’s Designated Safeguarding Lead and Deputy Lead have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.  As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in or out of school on a daily basis.

Canbury School believes that it is essential for parents / carers to be fully involved with promoting e-safety. We consult and discuss e-safety with parents / carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

#### Staff awareness

New staff receive information on Canbury School's e-Safety and Acceptable Use policies as part of their induction. All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policies which must be signed and returned before use of IT systems in school. Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

Any concerns staff have relating to e-safety must be reported as soon as possible to the school's Online Safety Coordinator and Designated Safeguarding Lead.

#### E-Safety in the curriculum and school community

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to students on a regular and meaningful basis. We look for new opportunities to promote e-safety and from time to time we monitor and assess our students' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, as well as informally when opportunities arise.

At age-appropriate levels, students are taught to look after their own online safety. They are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Students can report concerns to the Safeguarding Lead and the e-Safety Coordinator and any member of staff at the school.

Students are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Students are taught about respecting other people's information, including images, through discussion and classroom activities.

Students should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy). Students should approach the Designated Safeguarding Lead, Online Safety Coordinator as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

The school takes opportunities to engage parents in e-Safety matters, helping them to monitor and identifying risks and what mitigations they can employ.

#### Use of school and personal devices

##### Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked or they are logged out to prevent unauthorised access.

Staff at Canbury School are permitted to bring in personal devices for their own use and must comply with the School’s Mobile Phones/Devices Policy.

Personal telephone numbers may not be shared with students or parents / carers and under no circumstances may staff contact a student or parent / carer from a personal telephone number.

##### Students

In addition to the computers in the teaching rooms, Chromebooks, laptops and cameras are available for student to use and are stored in locked cupboards/drawers. Access is available via members of teaching and support staff. Members of staff should book the use of these resources for class use and while students are encouraged to take responsibility for taking and returning devices to their storage locations between lessons, staff should always check that all devices are returned for the next group of students to use them.

From September 2019 each year 7 & year 8 student is required to purchase a managed Chromebook for use in lessons and at home. These devices remain the responsibility of the child in the case of loss or damage but they are covered by insurance if purchased through the official school scheme.

If students bring in mobile phones, they should be kept switched off and out of sight during the school day, and will remain the responsibility of the child in case of loss or damage. They may be handed in to Reception at the start of the day and collected as they leave school or left in their lockers.

#### Use of internet and email

##### Staff

Each member of staff is issued with a managed G Suite for Education account that includes web based e-mail, collaboration and productivity tools. It is provided to support school work and activities. The account is not to be used for personal or leisure activities and its use can be monitored. The school's G Suite for Education accounts can be accessed in or out of school; communications are encrypted end to end and at rest and the service is individually password protected.

Staff must not access any website or personal email which is unconnected with school work or business from school devices whilst teaching or in front of students. Such access may only be made in staff-only areas of school.

When accessed from personal devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position (see the Social media policy for more details).

While the school employs end-point and gateway security measures on the managed school network all staff should take precautions against threats to school data associated with, and not limited to, phishing and scam emails, compromised websites and the use of personal portable storage media. Staff are made aware that email communications can be monitored.

Staff must immediately report to the Online Safety Coordinator 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 online communications must not either knowingly or recklessly:

* place a child or young person at risk of harm;
* bring Canbury School into disrepute;
* breach confidentiality;
* breach copyright;
* breach data protection regulations; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
	+ making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
	+ using social media or messaging to bully another individual; or
	+ posting links or material which is discriminatory or offensive.

Under no circumstances should school students or parents be added as social network 'friends'.

Any digital communication between staff and students or parents / carers must be professional in tone and content. Under no circumstances may staff contact a student or parent / carer using any personal email address. Staff should clearly separate their personal and professional lives when using technology and when online. The school ensures that staff have access to their school email account when offsite, for use whenever necessary on school business.

##### Students

Each Canbury student is issued with a managed G Suite for Education account that includes web based email, collaboration and productivity tools. It is provided to support each student's learning and must only be used for school work and activities. Students are made aware that the account is not to be used for personal or leisure activities and their use of these services is monitored. The school's G Suite for Education accounts for students can be accessed in or out of school; communications are encrypted end to end and at rest, and the service is individually password protected. The school employs end-point, gateway and service based security measures including web and email filtering. From time to time this may cause issues with legitimate school work or communication and in such circumstances students should speak with their teacher for assistance.

Students should immediately report, to the Designated Safeguarding Lead/Online Safety Coordinator the receipt of any communication or access to material that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not reply or respond to any such communication.

Students must report any accidental access to materials of a violent or sexual nature directly to the Online Safety Coordinator. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the school's Student Behaviour, Sanctions and Reward Policy. Students should be aware that all internet usage via the school's systems are filtered and monitored for inappropriate use.

#### Data Protection

Canbury school aims to adhere to the Data Protection Act 1998 and the GDPR of May 2018.  Please refer to the Data Protection Policy and the Acceptable Use Policies for further details.

Staff and students save all their work to the on-site school systems or their school G Suite for Education account. Staff are made aware of the data protection issues of saving local copies to their personal devices or home computers and are encouraged to use school provided systems, such as the remote access server or their school G Suite account where data is encrypted in transit and at rest.

USB memory sticks, writeable CDs, portable drives are not to be used in School. In circumstances where it is necessary to use removable media taken off site in person, or sent by post / courier the media must be encrypted at rest before leaving school premises. Members of staff should liaise with the IT Network Consultant for advice and guidance on how best to do this.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or students should ever be stored on personal devices, accounts, portable drives or memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Coordinator.

#### Password security

Students and staff have individual school network logins and G Suite for Education accounts and other authorised cloud based services such as RM Integris, MyConcern and others. Staff and students are regularly updated on the requirements for effective password security.

All students and members of staff should are encouraged to:

* use strong passwords - exceeding 12 characters or more and follow effective complexity rules
* not write passwords down
* not share the same passwords between different accounts
* not share logins and passwords with others.

#### Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming 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.

When using digital images, staff should inform and educate students 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).

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 on blogs or social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. Personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Students must not take, use, share, publish or distribute images of others without their permission.

Written permission from parents or carers will be obtained before photographs of students / students are published on the school website (see Parent Contract / Acceptable Use Policy for more information). Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

#### Reporting

While Canbury School encourages students and staff to talk openly about e-Safety issues there are often circumstances, such as inappropriate online behaviour, bullying and grooming, where a student is less comfortable to talk in an openly about their own experience. The school provides clear mechanisms for students to report these incidents either in person, by speaking in confidence with their preferred member of staff, or reporting via email to the DSL.

#### Filtering and Monitoring

Canbury School employs in-line web filtering at the school’s gateway to the internet and subscribes to a third party user monitoring system in order to monitor and alert Designated Safeguarding Lead and Head when e-safety incidents arise and a log of these incidents is maintained. Student Chromebooks are filtered and monitored by separate cloud based system that provides finer granularity of filtering of popular services such as YouTube.

#### Complaints

As with all issues of safety at Canbury School, if a member of staff, a student or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Online Safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or students involved. Please see the Complaints Procedure for further information.

Incidents of or concerns around e-safety will be reported to the school's Online Safety Co-ordinator and the Designated Safeguarding Lead in accordance with the school's Child Safeguarding Policy and Procedures and logged by the Online Safety Coordinator.