ST. CHRISTOPHER SCHOOL
LETCHWORTH GARDEN CITY

Whole School Policy on E-Safety & Cyber Bullying, including EYFS and After School Provision

November 2024

SECTION 1: Policy statement

1.1 The Governors and staff at St Chris are committed to providing a safe and happy learning environment, promoting equality and diversity and ensuring the wellbeing of all members of the community. It is their clear intention to promote good behaviour and to exercise their responsibilities in ensuring the safeguarding and welfare of all students and staff within the community.

1.2 This policy should be read in conjunction with the Conduct and Recognition Policy, Staff and Student Codes of Conduct, Boarding Handbook; and ICT Acceptable Use Policy.

SECTION 2: Scope of the Policy

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

2.2 The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Boarding School Behaviour Policy.

2.3 The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

SECTION 3: Roles and Responsibilities

3.1 Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

3.2 The Head has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the DSL and Pastoral teams.

3.3 The Head and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

3.4 The Head/Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

3.5 The Assistant Head (Pastoral Care):

- 3.5.1 Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- 3.5.2 Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- 3.5.3 Provides training and advice for staff.
- 3.5.4 Liaises with the Local Authority / relevant body.
- 3.5.5 Liaises with school technical staff.
- 3.5.6 Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- 3.5.7 Reports regularly to Senior Leadership Team.

3.6 Network Manager/Technical staff are responsible for ensuring:

- 3.6.1 That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- 3.6.2 That the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- 3.6.3 That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- 3.6.4 The filtering procedure is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- 3.6.5 That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- 3.6.6 That the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head/Senior Leader for investigation/action/sanction.
- 3.6.7 That monitoring software/systems are implemented and updated as agreed in school policies.

3.7 Teaching and Support Staff are responsible for ensuring that:

- 3.7.1 They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- 3.7.2 They have read and understood and signed the ICT Acceptable Use Policy (AUP).
- 3.7.3 They report any suspected misuse or problem to the Head/Senior Leader for investigation/action/sanction.
- 3.7.4 All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.

3.7.5 E-safety issues are embedded in all aspects of the curriculum and other activities.
3.7.6 Students understand and follow the e-safety and acceptable use policies.
3.7.7 Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3.7.8 They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.
3.7.9 In lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

3.8 Students are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy (AUP) and:

3.8.1 Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3.8.2 Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
3.8.3 Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
3.8.4 Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

3.9 Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

3.9.1 Digital and video images taken at school events.
3.9.2 Access to parents' sections of the website and on-line student records
3.9.3 Their children's personal devices in the school.

SECTION 4: Policy Statements

4.1 Education – students: Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
4.2 Education – Boarding: The school will provide opportunities for its local boarding community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

4.2.1 Providing courses in use of new digital technologies, digital literacy and e-safety to boarding staff
4.2.2 E-Safety messages targeted towards parents
4.2.3 As a boarding school, we have a community of boarding staff and their families that live on our school site. This group will be targeted as our wider community to allow better understanding within the whole boarding community of E-Safety issues.

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

4.3.1 A planned e-safety curriculum should be provided as part of Computing/PSHE/Design Technology and other lessons and should be regularly revisited
4.3.2 Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
4.3.3 Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
4.3.4 Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
4.3.5 Students should be helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school
4.3.6 Staff should act as good role models in their use of digital technologies, the internet and mobile devices
4.3.7 In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
4.3.8 Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
4.3.9 It is accepted that from time to time, for good educational reasons, students may need to research topics (eg. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.

Section 5: Technical – infrastructure/equipment, filtering and monitoring

5.1 The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

5.1.1 School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in Local Authority/other relevant body policy and guidance)

5.1.2 There will be regular reviews and audits of the safety and security of school technical systems

5.1.3 Servers, wireless systems and cabling must be securely located and physical access restricted

5.1.4 All users will have clearly defined access rights to school technical systems and devices.

5.1.5 All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password.

5.1.6 The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

5.1.7 Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

5.1.8 School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy.

5.1.9 An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.

5.1.10 Appropriate security measures are in place 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.

5.1.11 An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

5.1.12 An agreed procedure is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.

5.1.13 Staff should not use USB memory sticks at any time.

SECTION 6: Use of digital and video images

6.1 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 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:

6.1.1 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 eg. on social networking sites.

6.1.2 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. 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 students in the digital/video images.

6.1.3 Designated staff 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.

6.1.4 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.

6.1.5 Students must not take, use, share, publish or distribute images of others without their permission

6.1.6 Photographs published on the website, or elsewhere that includes students, will be selected carefully and will comply with good practice guidance on the use of such images. They will also only be used with the permission of the student and/or the parents/carers.

6.1.7 Parents or carers are informed and where appropriate consent is given for the school to use photographs of students on our school website.

6.1.8 Student's work can only be published with the permission of the student and/or parents/carers.

SECTION 7: GDPR and Data Protection

7.1 Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations which state that personal data must be:

7.1.1 Processed lawfully, fairly and in a transparent manner in relation to individuals.

7.1.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for

archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

7.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7.1.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

7.1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

7.1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.2 The school must ensure that:

7.2.1 It will hold the minimum personal data necessary to enable it to perform its function and it will not hold the data for longer than necessary for the purposes it was collected for. Please refer to Data Retention Policy.

7.2.2 Every effort will be made to ensure that data held are accurate, up to date and that inaccuracies are corrected without unnecessary delay.

7.2.3 All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.

7.2.4 It has a Data Retention Policy

7.2.5 It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

7.2.6 Responsible persons are appointed/identified - Data Protection Officer (DPO)

7.2.7 Risk assessments are carried out

7.2.8 It has clear and understood arrangements for the security, storage and transfer of personal data

7.2.9 Data subjects have rights of access and there are clear procedures for this to be obtained

7.2.10 There are clear and understood policies and routines for the deletion and disposal of data

7.2.11 There is a policy for reporting, logging, managing and recovering from information risk incidents

7.2.12 There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

7.2.13 There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

7.3 Staff must ensure that they:

7.3.1 At all times, take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

7.3.2 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.

7.3.3 Transfer data using encryption and secure password-protected devices.

7.4 When personal data are stored on any portable computer system, memory stick or any other removable media:

7.4.1 The data must be encrypted and password protected

7.4.2 The device must be password protected

7.4.3 The device must offer approved virus and malware checking software

7.4.4 The data must be securely deleted from the device once it has been transferred or its use is complete

SECTION 8: Cyber Bullying and Misuse of E-Systems

Treating Other Users with Respect:

8.1 The School expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the School's guidance on 'Respect for the Community' [copies of which are in the homework diary].

8.2 The School expects a degree of formality in communications between staff and pupils and would not normally expect them to communicate with each other by text or mobile phone. The School's policy on educational visits explains the circumstances when communication by mobile phone may be appropriate. In such circumstances, staff use School mobile phones (rather than their own); and pupil/staff phone numbers are deleted at the end of a visit.

8.3 Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The School's approach to bullying is set out in the Whole School Anti-Bullying Policy. The School is strongly committed to promoting equal opportunities for all, regardless of race, religion, sex, sexual orientation or disability.

8.4 All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or other worrying issue to a member of the pastoral staff, such as their Junior School teacher/Adviser/Personal Tutor.

8.5 The use of mobile phones is guided by the School's Mobile Device Policy.

SECTION 9: ICT in the curriculum

9.1 All pupils are taught core ICT skills through the PSHE programme. ICT has transformed the entire process of teaching and learning at St Christopher. It is a crucial component of every academic subject and the majority of the School's classrooms are equipped with electronic whiteboards, projectors and computers. St Christopher has a number of ICT suites and pupils may use the machines there, and in the library, for private study. All of the school's boarding houses are equipped with computers and network points.

9.2 St Christopher recognises that internet safety is a child protection and general safeguarding issue.

9.3 Our PSHE and Pastoral teams have expertise in the safe use of the internet, and the dangers involved in the misuse of ICT. Through both the PSHE and Pastoral programmes, all year groups in the School are educated in the risks and the reasons why they need to behave responsibly online.

9.4 Pupils of all ages are taught how to make use of the excellent online resources that are available from sites such as:

9.4.1 Safenetwork (www.safenetwork.org.uk)
9.4.2 Childnet (www.childnet.com)
9.4.3 Cyber Mentors (www.cybermentors.org.uk)
9.4.4 Cyber bullying (www.cyberbullying.org)
9.4.5 E-Victims (www.e-victims.org)
9.4.6 Bullying UK (www.bullying.co.uk)

9.5 Resources cover the many hazards encountered on the internet, and empower users with specific guidance, help and support.

SECTION 10: Considerate Use of Electronic Equipment

10.1 Mobile phones, smart phones, tablets and other personal electronic devices should be switched off and stored securely during the school day, in line with the Mobile Device policy, which is explained to pupils at the start of each academic year.

10.2 Staff may confiscate personal equipment that is being used during the school day in contravention of the policy.

10.3 Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

SECTION 11: Misuse – Statement of Policy

11.1 St Christopher will not tolerate any illegal material and will always report illegal activity to the police and/or the LSCB (Local Safeguarding Children Board). If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

11.2 Inappropriate Images appearing online

11.3 Children may be concerned that images of them (e.g. those hacked from Snapchat) have been uploaded to public websites. It is important that they are provided with support and know what to do if they lose control, particularly of a sexual image. It is never too late to get help.

11.4 Talk to a counsellor at ChildLine on **0800 1111** or at www.childline.org.uk. ChildLine will also work with the Internet Watch Foundation to notify sites hosting images to have them removed.

11.5 If young people are being harassed, threatened or blackmailed because of a sexual image they can report to us at CEOP via the CEOP report form at: www.ceop.police.uk/safety-centre

11.6 If images end up on a site children can often report to the sites where they have been shared.

SECTION 12: Cyber Bullying

12.1 Cyber bullying is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The School's Anti-Bullying Policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.

12.2 Proper supervision of pupils plays an important part in creating a safe ICT environment at school but everyone needs to learn how to stay safe outside the school.

12.3 St Christopher values all of its pupils equally. It is part of the ethos of St Christopher to promote considerate behaviour and to value diversity.

12.4 Bullying and harassment in any form should always be reported.

12.5 The children can do this using whichever method they feel most comfortable with:

12.5.1 In person to any member of staff: Junior School teacher/Senior School Adviser/class teacher/Head of Year/School Nurse/Head of Upper or Lower Junior School/Head teacher.by email: bullying@stchris.co.uk

12.5.2 To one of our major officials.

12.5.3 To the School nurse

12.5.4 Through Childline, whose phone number is posted around school.

12.6 It is never the victim's fault, and he or she should not be afraid to come forward.

Responsible and Accountable Persons	Name	Position
Responsible	Alistair Phillips	Assistant Head (Pastoral) and DSL
Accountable	Rich Jones	Head
Date Policy Approved	Approved by Governors 20 November 2024	
Review Period	Annual	
Review Date	November 2025	

Version History	Amendment Date	Amended by Whom	Previous Version Stored Where (If Applicable)
Previous version	February 2019	Gavin Fraser-Williams (Director of Pastoral Care)	Policy Archive Folder

Appendix A

FLOW CHART FOR RESPONDING TO INCIDENTS