SAINT CHRISTINA'S SCHOOL: ONLINE SAFETY POLICY including:

Review Initiated by	*Head teacher*
Reviewed	*Summer 2021*
Next Review	*Summer 2022*

Distribution: Policy Library on the Network.
Appendix 1: Staff Acceptable Use Agreement
Appendix 2: Student Acceptable Use Agreement

1. Introduction and Responsibilities

1.1. The internet and the use of digital media, is an essential part of education in the 21st Century. It is our aim as a School to provide appropriate and safe access to all that the internet and modern technology allows through the provision of modern and up-to-date ICT facilities. Responsibility for this safe provision is as follows:

- The Head teacher has overall responsibility for Online Safety within the School.
- The DSL is specifically responsible for online safety (See Child Protection Policy) and ensuring staff and students receive regular appropriate training and information.
- IT support is provided by I.T.CTRL Limited which has delegated responsibility for managing the IT infrastructure within the School, ensuring that the network and systems are used appropriately by all users and that safeguarding systems e.g. filtering etc., are fully functional.
- The SLT will help form and monitor Online Safety policy and strategy in conjunction with I.T.CTRL Limited.

1.2. Access to, and the effective use of, the internet within education, business and social interaction is an essential element of modern life. The internet is a rich resource for all sorts of information and its appropriate use should be encouraged to enhance teaching and learning. Increasingly students turn to the internet in the first instance in their search for resources or information. In addition, the internet is an important source of services used in everyday life, such as banking and social networking. Equally, it plays an important role in the administration of the School.

1.3. Alongside these opportunities there are risks attached to use. Distribution of material cannot be controlled whether that is an email or material posted on social media. Once distributed to an initial target audience, material can be shared anywhere through the networks of each individual in that audience and beyond. Information, including personal information can be harvested and misused. Internet Providers routinely retain data about sites used by its user's and organisations such as Google and Apple monitor online use for commercial reasons.

1.4. It is important to ensure that we consider the above in line with our duties in School, as well as our legal responsibilities, and our reputation. It is also important that we encourage an understanding that online activity is subject to all of the norms, protocols and regulations that apply to relationships in "real life".

1.5. The intention of this policy is to set out the ways in which the School will provide access to the internet with a view to ensuring staff and students are able to do this safely.

2. Internet Access for Teaching, Learning and School Administration

"Young people need to be able to determine which websites or other sources of information are reliable and which are bogus; to understand the dividing line between 'fun' and 'inappropriate' behaviour; and to grasp the risks they take in posting the pictures or comments online which they may come to regret, if not now then as adults and job-seekers in the future". (ASCL, The Impact of ICT, 2020 Future: Briefing Paper 4.)

2.1. School internet access is designed expressly for staff and student use and will include appropriate filtering.

2.2. Clear boundaries are set for the appropriate use of the internet and digital communications through Acceptable Use Agreements.

2.3. Children receive age appropriate specific Online Safety education within (IT lessons) and beyond the curriculum and staff receive appropriate training. The School also offers information to parents on Online Safety both through the sharing of important documentation and advice and in-School information evenings.

2.4. Students are (age appropriately) taught to be critically aware of the materials they read and are educated in the effective use of the internet for research, including the use of discrimination in the search for information and its retrieval.

2.5. Students are (age appropriately) educated that the use of internet derived materials by staff and by students must be legal.

3. Managing Internet Security

3.1. The security of the School's ICT system will normally be reviewed termly with the Bursar / Head teacher and I.T.CTRL Limited. I.T.CTRL Limited provide the School with a range of services that they directly provide or manage as part of a provision by a third-party. I.T.CTRL Limited works in partnership with any third party services that they supply in order to ensure that those services are up to date and appropriate for our School setting and will advise the School in this regard.

3.2. Virus protection is installed across the network and constantly updated. The School uses Avast for virus protection and updates are automatically applied across the network as they are released by Avast.

3.3. Filtering is provided by EXA Networks. EXA provide the School with a default filtering policy which is set at a strict level as appropriate for a Primary School setting. This is then tailored by I.T.CTRL Limited to allow for appropriate differentiation e.g. staff settings may be different to allow for greater internet use. The IT teacher also has the ability to 'white list' particular sites. In addition to this, network usage is monitored through the use of Securus software that captures and reports on activity that may raise concerns on the School network. Reports are passed to the School (Headteacher) by I.T.CTRL.

3.4. I.T.CTRL Limited is responsible for making regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable and take account of statutory responsibilities such as the need to protect children from radicalisation.

3.5. Staff and students will be encouraged to report any unsuitable website or web content that they discover to their class teacher or a teacher that they trust so that the ICT Support Manager can act on the information.

3.6. Security strategies will be discussed in the regular termly meetings with Bursar / Head teacher and I.T.CTRL Limited.

4. System Management

4.1. The computer system / network is owned by the School and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

4.2. The School reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

4.3. **Hardware:** I.T.CTRL Limited assist the School on the management and deployment of IT hardware. All hardware is set up for the School by I.T.CTRL Limited and advice is offered regarding replacement and upgrade.

4.4. **Staff:** I.T.CTRL Limited provide staff with login details for the network, Office 365 and G-Suite. When staff leave they will remove their accounts as directed by the School.

4.5. **Back up:** There is currently a 21 day retention policy for data that is backed up. The following data on the network is backed up offsite by Datalifeline every night (media data (video / photos etc., is not backed up within this regime):

- Oasis
- Pastoral
- Policy Library
- Premises
- SLT
- SMT
- Teacher folder – excluding Old Info Catch all folder
- Users Folder – excluding Leavers

Datalifeline Backup Provision is as follows:

a) Communications between the backup server and the School are transported in a 128-bit SSL (Secure Socket Layer) channel. Authentication parameters & encrypted files are further encrypted within an SSL.

b) Files are first zipped and encrypted with the School's defined encryption key before they are sent to the backup server.

c) The encrypting key used to encrypt School data is known only to School. Thus, even system administrators at Datalifeline cannot decrypt and view the content of files stored on the backup server without School permission.

d) The algorithm used to encrypt files is Advanced Encryption Standard (AES), with 256-bit block ciphers. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) in the USA for top-secret information. A 256-bit key size has 2256 or around 1.16 x 1077 possible combinations.
e) School can also restrict access to its backup files from the set of defined IP addresses. Access to School data from an IP address outside of the defined list will be denied.
f) Datalifeline Europe Ltd is registered with the Information Commissioner's Office (ICO) to fulfil our obligations under the Data Protection Act.

4.6. **MIS:** The School uses two MIS:

a) Oasis: is a discrete programme that sits within the School's IT framework. Oasis is backed up within the whole School back up regime.
b) Schoolbase: Data is maintained off-site and managed by Furlong Solutions who own and operate Schoolbase. Data is stored in compliance with UK Data Protection laws. Hourly and Daily backups are produced by a disk imaging process that takes a snapshot of the entire server from which we can restore any individual file. Weekly and Monthly backups are produced using SQL Server Agent.

5. Email / G Suite

5.1. Students are not given a School email account

5.2. All students are given a Google account as is needed by the Google Classroom environment. This is not an email account. It is a login for the Google Classroom environment (G Suite).

5.3. Staff are all issued with a School e-mail address, the use of which is encouraged for the smooth running of the School. All staff should be aware of and implement the separate School E-mail Policy which defines safe and appropriate use. See also the Staff Behaviour Policy. The School emails are provided within Office 365.

5.4. Staff are given a Google account in order to allow them to operate within the Google Classroom environment.

5.5. Online contact between staff and students is allowed through the Google Classroom and can be monitored. Direct email contact is not permitted.

6. Social Networking

6.1. The School will control access to social networking sites via the School network and educate students in their safe use as part of online safety education. Social networking sites will not normally be accessible unless a specific use is approved.

6.2. Students will be given Online Safety guidance on safe internet during their time at the School. This will include:

a) Advising students that they should not give out personal details which may identify them, their friends or their location.

b) Advising students and staff that they should not place personal photos on any social network space without considering how the photo could be used now or in the future.
c) Advising students and staff that they should only invite known friends and deny access to others when using social networking and instant messaging services.
d) Making students and staff aware of the need for security and the importance of setting passwords to deny access to unknown individuals and to block unwanted attention and communications.
e) Making students (age appropriately) and staff aware of the Child Exploitation and Online Protection Centre (NCA's CEOP Command) and the 'Report Abuse' links that exist on most social networking sites.

7. Published content and the School web site

7.1. The point of contact on the Website is the School address, School email and School telephone number.

7.2. Staff or student personal contact information will not generally be published. Any contact details given online should be those of the School office.

7.3. The Head teacher will take overall editorial responsibility and ensure that published content is accurate and appropriate.

7.4. The School reserves the right to include photographs and images of students in the School's promotional material where a parent has not withheld consent (refer to the photo consent procedure and the list of students whose photograph should not be taken for promotional purposes – list available from the School Office). We would not disclose the name of a child without the parents' consent. This policy is consistent with the Terms and Conditions that all parents agree to when their son or daughter joins the School.

7.5. Photographs that include students will be selected carefully with a view to our responsibilities for their safety and well-being.

7.6. Work produced by students may be published on the website and in other School publications.

8. Managing Emerging Technologies

8.1. Emerging technologies will be examined for their educational benefit and assessed before use in School is allowed.

8.2. Technologies such as personal mobile devices with internet access are not part of the School network and are able to bypass School filtering systems and present a new route to undesirable material and communications. It is not possible to monitor this activity with the resources that are currently available to the School.

8.3. Personal mobile devices are not allowed in School and where parents would like their child to bring a personal mobile device to School, e.g. their child is in Year 6 and walking

to School, they must first notify the School and the device must be handed into the School Office by the child, on arrival at School.

8.4. The School understands that children do have access to personal mobile devices outside of School and that they therefore need to be educated to use them appropriately and safely. The School will be proactive where it is aware of issues around this e.g. the sending of abusive or inappropriate text messages, online bullying, or the posting of inappropriate images. Such behaviour will be dealt with as serious matters.

8.5. School provided tablets or mobile devices will only be used during lesson or formal School time when permission is given and use is supervised by a member of staff.

9. Protecting Personal Data

9.1. Details about how the School manages and protects personal data can be found in the Data Protection (GDPR) Policy.

9.2. The School maintains CCTV as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation. See the Data Protection (GDPR) Policy

10. Policy Decisions authorising internet access and ensuring safe use

10.1. Staff must agree to the Staff Acceptable Use Policy in order to use the computer network.

10.2. Students must agree to the Student Acceptable Use Policy in order to use the computer network. Understanding the Student AUP forms part of the first week of IT lessons within the School year.

10.3. The School will maintain a current record of all staff and students who are granted access to School IT systems.

10.4. Parents will be asked to sign the Student Acceptable Use annually, to show that they understand and are in agreement with the terms of usage.

10.5. The School will take all reasonable precautions as outlined in the section on Managing Internet Security (see above) to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content it is not possible to guarantee that unsuitable material will never appear on a computer connected to the School network. The School cannot accept liability for any material accessed, or any consequences of internet access, although it will do all that is reasonably possible to reduce the risk of inappropriate material being accessed.

10.6. The AUPs make clear that staff and students must always keep their password private and must not share it or leave it where others might find it.

10.7. The AUPs makes clear that no one should log on as another user and that students should never be allowed to logon or use teacher and staff logins as these have different security restrictions and might enable access to confidential information, amongst other things.

10.8. Saint Christina's School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.

10.9. The School has set-up the network with a shared work area for students and another for staff. Staff and students are shown how to save work and access work from these areas.

10.10. The AUP requires all users to always log off when they have finished working or are leaving the computer unattended; where a user finds a logged-on machine, we require them to log-off and then login again as themselves.

10.11. The School has set-up the network so that users cannot download executable files / programs.

10.12. All computer equipment is installed and maintained professionally by I.T.CTRL Limited and meets health and safety standards e.g. projector filters cleaned, equipment installed and checked by approved Suppliers / electrical engineers, annual PAT (Portable Appliance Testing) etc.

10.13. The School's wireless network has been secured to appropriate standards suitable for educational use. All computer equipment is installed professionally and meets health and safety standards.

10.14. The Head, the SLT and the IT teacher, as appropriate, will ensure that the implementation of the Online Safety policy is appropriate and effective.

11. Handling Online Safety complaints

11.1. Complaints of internet misuse by students will be referred to the child's class or IT teacher (if appropriate) and brought to the attention of a member of the SLT in the first instance.

11.2. Any complaint about internet misuse by staff will be referred to the Head or the Deputy Head where the Head teacher is not available. The Bursar will deal, in the first instance, with any complaint about the misuse of the internet, by support staff. The Head will be informed where this is the case.

11.3. Complaints of internet misuse or relating to safeguarding will be dealt with as appropriate and in accordance with prevailing School policy e.g. Child Protection and Safeguarding Policy, Complaints Policy, Staff Behaviour Policy, HR policies – Discipline etc.

12. Communicating Online Safety

12.1. In order to create an environment where Online Safety is instinctively known and understood we intend to educate the whole-School community. In this we include parents and governors.

a) Students

- Online Safety information is permanently communicated through a lively and relevant display within the IT room. Other displays may be placed outside the IT room from time to time. Other relevant information will be displayed in classrooms. This communication is overseen by the IT teacher and, if relevant, the Deputy Head (DSL).
- All users are made aware that network and internet use is monitored although many of the children are very young and therefore will need things to be explained in an age-appropriate way. Parents are asked to explain the AUP to their child as part of signing that agreement.
- Students will be taught about the safe use of the network and internet. Most use will be within an approved environment such as a particular learning platform. Use of internet browsers for reason of research, for example, will always be managed in an age-appropriate way and supervised.
- A programme of training in Online Safety will be delivered across the whole School through the curriculum and more broadly, as appropriate to age and section, making use of appropriate materials.
- The School fosters a 'no blame' environment that encourages students to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable. They are taught, in addition, to switch off their monitor whilst the matter is dealt with by the teacher.
- Within the curriculum, each September the first week at School is designated to Online safety. The children are reminded about the right and safe use of IT and they all receive a copy of the student AUP to take home and sign with their parents. All students are taught how to report abuse and how to recognise and respond to cyber-bullying.
- Parents also sign the Google agreement in recognition of the fact that students have their own account within the Google Classroom environment. This is used to varying degrees across the School depending on age.
- The School uses 'Online Safety Week' and 'Anti-bullying Week' to emphasise aspects of safety and very often links up with an organisation such as the NSPCC to support the message and the delivery of the message. Lessons during these weeks reinforce good practise.
- Whilst we do not have CEOP trained staff in School both the IT teacher and the Deputy Head (DSL and responsible for online safety) are part of the Camden safeguarding group. This gives the School access to CEOP trained professionals (e.g. Mary Rebelo (CEOP Ambassador)) who are able to advise and help deliver our online safety talks.
- The School has access to CEOP trained personnel to advise and help deliver Online Safety training.
- The Acceptable Use Policy will include advice on how to stay safe on the internet.

b) Staff

- All staff will be made aware of the School's Online Safety Policy.
- Staff are informed that network and internet traffic is monitored and can be traced to the individual user. I.T.CTRL Limited provide IT services to the School and will work closely with the School to ensure that the School is fully informed regarding the infrastructure that they deliver and manage. I.T.CTRL Limited will inform the School where there are problems and provide regular reports and updates, as required, on use, present dangers etc.
- Staff will receive Online Safety training and updates.
- Staff should only use the School IT provision for work-related activities.
- School colleagues are asked to exercise caution and professional judgement about how they use their own personal social media accounts outside of School, what they use them for, and who they communicate with. Colleagues are advised to make full use of the security settings available within the devices that they use but note that these cannot be guaranteed to provide protection against allegations being made or disciplinary action being taken. Staff should not have current or recent parents (or students) as friends on social media. (See also the Staff Behaviour Policy).
- The School maintains a number of social media accounts for the purpose of presenting information about the life of the School to current and prospective parents. This is managed by Staff given responsibility for marketing. They will be mindful of the 'rules of engagement' as outlined in the section of this policy on 'Published content and the School web site'. The School's social media accounts may not be used for personal postings.

c) Governors

- The Board of Governors is aware of the School's Online Safety policy and strategy which exists with its approval.
- Governors will be invited to attend and receive Online Safety training as members of the School community. This will be refreshed as appropriate.

d) Parents

- Parents will be made aware of the School's Online Safety Policy through School publications and mailings.
- Relevant Online Safety material will be made available to parents with a view to educating them as members of the wider School community and with a view to ensuring safe use of the internet at home as well as in School. Information will be shared with parents from time to time and as issues, strategies and policies emerge nationally.
- The School arranges for regular online safety talks for parents. These are currently delivered around the national 'Online Safety Week' or 'Anti-bullying Week' by a CEOP Ambassador from the Camden Learning Centre (used as part of the IT teaching programme).

Related policies and documentation

Anti-Bullying Policy
Behaviour Policy
Child Protection and Safeguarding Policy
E Mail Policy
ICT Acceptable Use Agreements (AUP) (below)
Staff Behaviour Policy

Sources

BECTA
EXA – Surf Protect
Furlong Solutions
NCA's CEOP Command www.getsafeonline.org
Childnet, ThinkuKnow
Julia Codman, CEOP and Sheffield Safeguarding

Appendix 1

Saint Christina's School – Acceptable Use Agreement (Staff)

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct. Members of staff should consult the School's Online Safety Policy and the Staff Behaviour Policy for further information and clarification. You must not use any ICT on-site until you have signed this Code of Conduct document and logged it with HR.

- I will respect all ICT equipment/facilities at Saint Christina's School and will report any faults that I find or any damage that I accidentally cause to the ICT Co-coordinator.
- I agree to abide by this policy in respect of any of my own ICT equipment or personal mobile devices that I bring on site. If any ICT device (personal or School-issued) is being used inappropriately or illegally on site, this will result in disciplinary action.
- I understand that no photographs of students or their personal data may be taken with or stored on my personal electronic devices, including personal computers.
- I understand that personal mobile devices may not be used, come into or be stored within the EYFS setting (separate locked storage is available to staff).
- I agree to ensure that personal mobile devices are kept securely within School so that they cannot be accessed by children.
- I agree that personal mobile devices may not be used in any part of the School where children are present or routinely have access.
- I will not allow unauthorised individuals to access School email, Internet, the School network /other School systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the School's network and data security and confidentiality protocols, deleting data securely which is no longer necessary.
- I will only use the approved, secure email system(s) for any School business.
- I will only use the approved School email or other School approved communication systems with students or parents/carers, and only communicate with them on appropriate School business.
- Photos of students will not be uploaded to personal social media accounts.
- I am familiar with the School's Data Protection Policy and I agree I am responsible for the security of all personal data in my possession. I agree that any personal data that relates to an identifiable person is kept locally on the School's secure servers and will not be taken off site unless absolutely necessary. If data is taken off site, a removable memory device will be used which is encrypted or contained within password-protected files to prevent unauthorised access.
- I agree and accept that any iPad, computer or laptop loaned to me by the School, is provided to support my professional responsibilities. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow School data security protocols when using any such data at any location.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others, or I suspect a data breach, then I will immediately report this to the Data Protection Officer, Joanne Reilly. (See Data Protection Policy for further details).
- I agree that my use of Saint Christina's School ICT equipment/facilities will be monitored for safeguarding purposes. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using Saint Christina's School equipment/facilities. I understand that I may temporarily access blocked websites, services and other online resources using only tools that are provided by Saint Christina's School. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.

- I agree that the provision of Saint Christina's School ICT equipment/facilities including the email and Internet system are for educational purposes, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on-site or using Saint Christina's School equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the School's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not deliberately view, send, upload or download any material that is unsuitable for the School environment whilst I am in that environment or using any ICT equipment/facilities belonging to Saint Christina's School. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the Headteacher, Bursar or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve Online Safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the Headteacher, Bursar or senior colleague. I will not access any material that senior staff have rated as unsuitable.
- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using Saint Christina's School equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold Saint Christina's School responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with students through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the School email system may be used.
- I will use a School mobile phone to contact parents and students as necessary on School outings or when offsite with students.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the School's current Staff Behaviour, Safeguarding and Online Safety policies.

I agree to abide by all the points above.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the School's ICT resources and systems.

Signature ..... Date ……..

Full Name …….. (printed)

Role (Job title) ……

APPENDIX 2

Saint Christina's School - Student Acceptable Use of ICT Agreement

We want each student to enjoy using ICT and the internet, and to become proficient in drawing upon them both during your time at School, and as a foundation for your further education and career. To ensure your safety, you must agree to the following statements to allow you access to ICT at Saint Christina's School:

Please read this document together with your child and sign and return it on the first day of School. No child will be permitted to use the School network without having done so.

We expect that students will follow the guidelines. For their additional protection, we have installed content-filtering software and monitor all Internet access. The content filtering software is designed to prevent any accidental or intentional access to inappropriate material on the internet. Despite the School's best efforts, if any unsuitable sites are accessed through the internet, they are to be reported immediately and will be added to the updated filter list. The School explicitly addresses the issue of Online Safety for students in the ICT curriculum. The following guidelines should be adhered to whenever students are working on the School network. The principles of safe use are also applicable to student use of IT outside of the School and apply to home learning and the Google Classroom (G Suite) facility that is used by students from time to time. We want our students to grow up safely in their use of IT and so would urge the principles of safe use to also be applied in their personal use of IT too.

Guidelines for Internet and Local Network Access at* Saint Christina's School*:

- I will only use electronic devices in School for School purposes and will not use them for personal or recreational use unless I have permission to do so.
- I will handle all computer equipment carefully and will not touch power/network cables, or eat and drink in the IT suite or near IT equipment e.g. IPads / Chromebooks.
- I will not use disks, memory sticks or any other hardware with School equipment without the permission of my teacher.
- I will not connect a personal device (laptop, mobile device) to the School network without the consent of the Headteacher, Bursar or Deputy Head.
- Students are not allowed to have personal mobile devices within School and may not use 3/4/5G connections at School, which will bypass School filtering systems.
- I will not attempt to disable or circumvent any of the School's security/filtering systems.
- I will not download or install software on School equipment.
- I will only log on to the School network and other systems with my own user name and password.
- I will not reveal my passwords to anyone other than my class teacher and will change them regularly.
- I will make sure that all electronic communications e.g. within the Google Classroom (G Suite) with students, teachers or others is responsible, polite and sensible.
- I will not deliberately browse, save or send material that could be considered offensive or illegal, if I accidentally find anything like this I will tell my teacher immediately.
- I will not publish any personal information such as my name, phone number or address.
- I will ensure that my online activity, both in School and outside School, will not cause distress to my School, the staff, students my parents or others.
- I understand that all my use of the Internet and other related technologies can be monitored and logged for my safety and protection and can be made available to my teachers.
- If I see other people misusing IT equipment within School I will report it to a teacher.
- My parent/carer and I will sign and return the School Acceptable Use Policy.
- I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/ carer may be contacted.

Acceptable Use of ICT across the School

Students are expected to use the School ICT systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All use, however, should be consistent with the School ethos and code of conduct, and with the Internet and Local Network Acceptable Use Guidelines. The following list does provide some examples that must be followed:

- I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the School into disrepute.
- I will not read other people's communications without their consent.
- I will always be polite and courteous when communicating with others using IT just as I would if spoke to them in person. I will always use polite and appropriate language.
- I will not say or communicate things (e.g. by finding things online and sharing them) that could radicalise, or stir up hatred against any individual, ethnic, religious or other minority group.
- I will not reveal any personal information (e.g. home address, telephone number) about myself or other users on the School network.
- I will not use other people's login details to view or post anything on the School network.
- I will not share my login details (including passwords) with anyone else, apart from my parents/carer.
- I will ensure that if I think someone else has learned my password then I will change it immediately and/or contact the IT teacher or my Class teacher.
- I will ensure that I log off after my session has finished.
- If I find an unattended machine logged on under other user's username I will not continue using the account – I will log it off immediately and inform the IT teacher who will remind the person re safety in the future.
- I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to the School ICT coordinator.
- If I believe personal data may have been compromised (this means that people who should not have access to it, may be able to access it), or has already been accessed by others, I must report this to a member of staff immediately as it is potentially a very serious problem.
- I will only use cameras or other recording devices with permission from a member of staff and those appearing in the image. These photos may not be uploaded to social media or other websites by a student.
- I will only communicate with members of staff in person or the Google Classroom if that is appropriate. For my own safety I should never have the personal contact details of any member of staff.
- I realise that students whose use IT may be suspected to be inappropriate may have their usage closely monitored. All activity on the School network is logged and can be investigated if there is need to do so.
- I will not receive, send or publish material that violates copyright law.

Unacceptable Use

Examples of unacceptable use include, but are not limited to:

- Logging in to the School network with another person's user name and password, or using a machine left unattended with another user logged into it.
- Creating, transmitting / sharing, displaying or publishing any material (e.g. text, images, videos or sounds) that is likely to upset, bully, waste time or cause anxiety to any other person.
- Activity that would spoil, damage or delete another person's work or which might hurt the privacy or dignity of another person.

Google Apps for Education (G Suite)

Google Apps for Education is a set of online tools for teaching and learning, communication, collaboration, and document storage. All of these tools are housed on the Internet and can be accessed from any Internet-connected device with a web-browser. They form the School's VLE (Virtual Learning Environment). No special software is required. The G Suite comprises: Google Drive for storage, Google Classroom for the setting and

assessment of work or communication of teaching materials (videos, links to online material) and Google Meet which allows for live online teaching within a virtual classroom.

Our primary reasons for supplying these tools to students are:

- To supplement classroom teaching and to facilitate effective completion of homework.
- To help students work collaboratively and engage in peer-editing of documents.
- To enable efficient document storage and transfer from the School's iPads / Chromebook should this be appropriate.
- To maintain online access to useful teaching resources for parents and students e.g. phonics videos and other useful Library material (EYFS).
- To ensure that all students are able to access online teaching through an exceptional period such as prolonged illness or as has recently occurred, the enforced shut down of the School.

The School provides students with a Google Apps for Education account which includes a School email and password. The School will also be providing a step-by-step guide to use the Google Classroom teaching platform (G Suite).

Whilst the School has chosen the Google platform for its online provision and whilst this is, for safety reasons a 'closed platform', i.e. it is open to signed up School members only, when accessed from home students should only be online when parents are aware; that they are in a public space or area within the home; and that there is appropriate oversight for the age of the child.

Use of the G Suite forms part of the student AUP agreement that all students and parents sign to enable use of. Whilst much of the AUP relates to use within School, the general principles laid within the agreement around the 'right' use of IT apply even where we are teaching and learning remotely.

By signing the student AUP you agree to the School supplying your child with a Google Account as described.

✂----------

<u>Parental Agreement: Student AUP and use of IT at Saint Christina's School</u>

Pupil name: …… Class……..…

As the parent or legal guardian of the above pupil, I grant permission for my daughter or son to have access to use the Internet and other ICT facilities at School.

I have read and understood the student AUP. I understand that the School explains the AUP in an age-appropriate way and have spoken with my child to make sure that they understand the rules and guidance included. I consent to the School creating a Google App for Education (G Suite) account for my child with a view to enabling them to have access the School's Virtual Learning Environment (VLE). I consent to my child's use of the School IT network and equipment and am aware of the School's Online Safety Policy which is maintained on the School website, within various publications and which can be obtained on request from the School Office.

I know that my daughter or son has signed an Online-Safety agreement form and that they have a copy of the Saint Christina's School Online-Safety Rules. I will discuss the importance of these rules and support my child to use the School's ICT facilities appropriately.

I accept that ultimately the School cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the School will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include

using an educationally filtered service, employing appropriate teaching practice and teaching Online Safety skills to pupils.

I understand that the School can check my child's computer files, and the Internet sites they visit and that if they have concerns about their Online-Safety or e-behaviour that they will contact me.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my child's Online-Safety.

Parent / Guardian name(s) …….....

Parent / Guardian signature: …….. Date: ……

APPENDIX 3

Saint Christina's School - KS1 / EYFS Agreement/Online-Safety rules

- I will use technology in school only for learning and studying.
- I will not share my passwords with anyone.
- I will only delete or open my own files.
- I will make sure online communication with other pupils and adults is polite and responsible.
- I will not use my computer to send children or adults anything which is unpleasant or upsetting. This might be pictures or a video or it might just be unkind words. If I find anything like this on the screen, or if somebody upsets me, I will tell my teacher straight away.
- I will not tell people I don't know, my name, phone number or address when I am on the computer.
- I will not speak with someone on my computer unless it is someone part of a School project and my parent, or a trusted adult such as my teacher, is with me to make sure I am safe.
- I know that my computer is looked after and monitored by the School and that my parent/carer will be contacted if a member of School staff is concerned about my Online-Safety.

APPENDIX 4

Saint Christina's School – SMART Rules for Staying Safe Online

Safe

Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you don't trust online…

Meeting

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only if you really need to and when your parents or carers can be present...

Accepting

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages! If you are not sure, don't open and delete.

Reliable

Someone online may be lying about who they are, and information you find on the internet may not be reliable... You need to use your brain in deciding whether or not something is safe or trustworthy. If in doubt, ask your parent, carer or trusted adult before you do anything.

Tell

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at:www.thinkuknow.co.uk...