Whole School Information and Communications Technology (ICT) Policy - Guidelines for the Use of Digital Technology

The Whole School refers to all staff and students in the St. Catherine's Preparatory and Senior Schools which includes: the Early Years/Foundation Stage (EYFS), Pre-Prep School (Key Stage 1), Prep. School (Key Stage 2); Middle School (Key Stage 3); Senior School (Key Stage 4) and the Sixth Form (Key Stage 5).

History

This policy was first implemented in 2002 with subsequent revisions in 2005, 2008, 2009 and 2011. This version of the Policy written in 2013 and reviewed in 2016 takes into account further regulatory changes, and the 'Bring Your Own Device' policy of the School. This policy has been developed with reference to and in line with The Use of Social Media for Online Radicalisation 2015 and KCSIE (DfE 2016).

It should be read in conjunction with the following:
Child Protection Policy
Anti-bullying and Anti-bullying in the Workplace Policy
Code of Conduct for Staff
Confidentiality and Data Protection Policy
Classroom Guidelines for the use of iPads

Digital Technology at St Catherine's School

St Catherine's School avidly supports and encourages the use of digital technology in teaching and learning, in the classroom and in private study by pupils and staff alike. We have always taken great pride in keeping up-to-date with the latest technology in the classroom and are now embracing tablet technology that is revolutionising the way education is delivered around the world. We are proud to be at the forefront of this transformation.

This policy includes guidelines for everyone: students, teachers and parents. During the school day, teachers will guide pupils towards appropriate materials. Outside school, families bear the same responsibility for such guidance as girls interact with information sources such as television, films, radio and the internet including the use of social media.

Information and advice on e-safety for parents can be found on the Community page of our website which requires a username and password published regularly to parents. These materials are reviewed regularly and updated as required. Information regarding online safety and mobile device safety is also published to parents via iTunes U. Parents are notified of updates in the start of term policies email or by separate ClarionCall.

Aim: To promote the successful and safe use of digital technology and to enhance teaching and learning at all levels.

ICT Development

The Management of ICT in School is undertaken by the ICT Development Committee which holds meetings on a termly basis. This is a cross-phase group with academic and ICT staff from both Schools in attendance, a member of the administrative staff, and two governors. When necessary, senior pastoral staff are invited to attend when pupil welfare is discussed. Other staff are invited if a particular area of expertise is required in key discussions.

Aims of the Information and Communications Technology (ICT) Development Committee
- To create and maintain an ICT provision for staff and students to support teaching, learning and administration which will make St Catherine's a centre of excellence.
- To devise and oversee a whole school ICT strategy which foresees future developments and offers financial budgeting which governors can trust. Financial projections should manage funds appropriately and effectively.
- To be aware of the safeguarding responsibility of the school with regard to ICT and oversee the provision of guidelines for the use of digital technology.
- To prioritise appropriately the way ICT developments take place.
- To be responsible for the management of all the implementation and installation of ICT facilities, to oversee the School's Bring Your Own Device (BYOD) strategy and support the use of personal devices.
- To be representative of the whole school on both sites and have a whole school view of the development of ICT.
- To offer widespread ICT access and appropriate training to enable staff to be secure, enthusiastic and skilled users.
- To ensure that all staff are encouraged to become confident and regular users of the school's Information Management System (SIMS) as an educational tool.

Reviewed by the ICT Development Committee 11th May, 2015

ICT Provision

St. Catherine's School provides a sophisticated ICT infrastructure in order to give our pupils and staff the opportunity to use the best resources available for teaching and learning. Each pupil from Upper 2 to Upper 5 is required to bring an iPad to school to support their education.

The ICT infrastructure incorporates the following:

- 10Gb fibre links to all outlying building across senior and prep school sites supporting a 10Gb switching backbone and delivering 1Gb to each workstation.
- Virtualised server infrastructure with redundant systems and backup replication.
- Enterprise grade Wi-Fi solution covering the Senior and Prep School sites
- Application aware 'next generation' firewall providing year group based internet filtering and permissions which delivers daily reports on internet usage.
- MDM system used to deliver profiles and chosen apps to pupil owned iPads.
- Apple & PC based workstations to provide a comprehensive education in commonly used IT systems.
- Projectors and Interactive Whiteboards and Apple TVs in a vast majority of classrooms.

Each member of teaching staff and pupils from Upper 2 to Upper 6 is provided with a school login, email address and Google Apps account. Pupils under the age of 13 require written permission from their parents to use a Google Apps account. Staff and pupils also have access to individually permissioned shared areas used and the use of a personal documents area.
Pupils: Instructions given via ICT lessons, Life Matters, and training on use of digital technology (iPads), and through general education: assemblies and tutor time. Sanctions are detailed in the relevant Rewards and Sanctions and Anti Bullying policies.
Staff: Training in safeguarding including PREVENT, INSET including use of technology in the classroom,
Parents: emails/letters/ presentations by outside experts. When visiting the school parents are given basic access to the internet as an Upper 3 pupil which allows them to access their email account and the internet with all the firewalls in place.
Staff, pupils and parents sign IT agreement.

The members of the ICT Support Department and E-Safety Team are as follows:

2

Name	Position	Responsibility
Dan Raymond	Director of Digital Technology	Overseeing all aspects of the ICT Provision at St Catherine's School
Stephen Pink	Lead IT Technician	Support of IT systems and IT technicians
Matt Coppinger	Apprentice Technician – IT and Ann Halls	Support of IT systems and Anniversary Halls
Jack Matthews	IT Technician	Support of IT systems.
Davina Byrne	Head of Curriculum ICT	E-Safety
Kay Chaventre	Director of E-learning (Prep School)	E- Safety (Prep School)
Laura White	Coordinator of Digital Learning	Use of technology for teaching and learning

The school employs a CCTV system of 30 external HD cameras connected to the IT system. Access to footage is restricted via a password and required software, and overseen by the IT Support department.

Guidelines for the use of Digital Technology by Students Inside & Outside School

Part 1 – School Owned Digital Technology & Acceptable Use

Hardware, software and network resources purchased or provided by the School are to be used for creating, researching and processing school-related materials. The whole School is responsible for exercising good judgement regarding the reasonableness of personal use. Storing personal files such as music, digital pictures and video on the School system is not permitted. By using the School's hardware, software and network systems pupils/staff assume personal responsibility for their appropriate use and agree to comply with this policy, as well as applicable laws and regulations. For Prep. School pupils, this responsibility is taken by the supervising member of staff.

School Computers and Internet Access

- School computers and internet access are predominantly for the use of teaching and learning. Limited personal use of e-mail and internet is acceptable but this must not interfere with the staff or students' work. Unreasonable personal use may amount to misuse of the facilities.
- Computers and associated equipment must not be tampered with in any way.
- Any faults with computers should be reported as soon as possible to a member of the IT Support Department. It.support@stcatherines.info
- Executable files or files of any type that could cause damage to the School system may not be downloaded on to the network.
- It is all users' responsibility that any USB keys used on the School computers have been scanned for viruses. The IT Support Department can provide assistance if required.
- Prep. School girls must always ask a teacher's permission before using a computer or mobile device.

School Email System

The School provides an email system that is accessible to all members of staff and senior school students. Prep school pupils in Upper 2 and Lower 3 are provided with a school e-mail address for internal use only. Staff and senior school students must use the School's system for email to students or parents, and not personal email accounts. Email accounts may be set up on personal mobile devices to enable receipt of school emails whilst on or off the School premises if desired. Helpsheets are available on configuration from the IT Support Department.

Users should not use the School's email for participation in chain letters, soliciting for charitable endeavours, either their own or on behalf of others, or distributing material which violates or infringes the intellectual property rights (including copyright, patent or trademarks rights) of any other person or organisation (including the School). The School wheel logo is a Registered Trademark. Permission for its use beyond school must be granted by the Headmistress.

Any email sent out using the School's server will be sent from the School and may therefore impact upon the reputation of the School. In the same way, accessing the internet from the School network means that it is the School accessing the site, not just the user in a personal capacity.

School staff should follow advice outlined in the Staff E Mail Charter in the Staff Handbook.

Printing
St Catherine's is an 'eco-school'. As such, we believe in the 'green' use of IT and feel strongly that the whole School should only print if absolutely necessary. ***'Think before you print!'***
The School uses print management software, 'Papercut'. Each member of staff and each Senior School student is provided with a 'Papercut' number. This will enable the release of print jobs only when you are logged in to a 'Papercut' enabled printer.

Senior School students receive a monthly quota of print credits. Should girls require additional credits, they must make a request to the IT Support Department. Prep School girls must always ask permission before printing work.

Only paper which has been supplied by the School should be used in the printers. Authorization must be obtained from the IT Support Department if girls wish to use any other form of printing media.

Wireless Network
A wireless network is provided across Senior and Prep School sites. Personal laptops and mobile devices may be configured for use with the wireless network with the help of IT support. Help sheets and assistance with configuration are available from the IT Support Department.
Parents, boarding families and visitors to the school are kept on separate wireless networks from the staff and student devices, for personal and data security. All wireless networks are protected by unique passwords. Access to the Internet from guest networks is restricted to a basic level and protected by the school firewall. Internet access for all purposes is reviewed regularly by the IT Support department and the ICT Development Committee.

Part 2 –Internet Use
The School may exercise its right to monitor the use of its computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials where it believes the School's computer system is being used inappropriately. All users have prescribed internet permissions that apply whilst accessing the internet whether through a mobile device or a school computer.

In line with our aim to keep children safe from radicalisation and exposure to terrorist and extremist material, the school additionally monitors and reports on related online activity. The level of monitoring and filtering is under constant review.

Blocking and barring of sites does not guarantee protection.
When girls are provided with 3G/4G enabled devices – in particular phones - the School cannot guarantee protection from inappropriate websites. The ultimate protection is in the good sense of young people knowing what is available to them and the risks to which they may be subject. This principle is embedded in our curriculum and girls in each age group are taught about internet safety at an appropriate level which is built upon as they progress through the school.

Social Media Guidelines
The term "social media" encompasses social networking sites such as, but not limited to, Facebook, MySpace, Instagram and Twitter, as well as to more general types of social media such as, but not limited to, blogs, wikis, podcasts and digital images/videos.

Personal Responsibility
The lines between public and private, personal and professional can easily become blurred in the digital world.
- Staff and girls are personally responsible for the content they publish online. Users should be mindful that what they publish will be published for a long time. Future employers could access

4

even your earliest Facebook pages. Publishing any material that defames the school will always be dealt with as a serious disciplinary matter.

- Online behaviour should reflect the same standards of honesty, respect, and consideration that is expected when conversing face-to-face. What is inappropriate in the classroom should be deemed inappropriate online.
- When contributing online, do not post confidential or personal information.
- Comments made on sites such as Twitter are not protected by privacy settings. The St Catherine's Community should be aware of the public and widespread nature of such media.
- By posting comments, having online conversations, etc. you are broadcasting to the world. Be aware that even with the strictest privacy settings what is 'said' online should be within the bounds of discretion. Comments expressed via social networking pages under the impression of a 'private conversation' may still end up being shared in a more public domain, even with privacy settings on maximum.
- Before posting photographs and videos, permission should be sought from the subject where possible. Staff posting photographs of girls on the School website for news or PR purposes should check that they do not feature any girl for whom permission has not been granted by her parents for photographs to be used. No photograph of a girl on the public section of the website will be named.
- Before posting personal photographs, thought should be given as to whether the images are appropriate.
- Communication via social media is overseen by Director of Digital Technologies and Senior Housemistress. Personal connections between student and staff social media accounts are not allowed.

Disclaimers

The St Catherine's School community must include disclaimers within any personal blogs that the views are the writer's own and do not necessarily reflect the views of the School. For example:

"The postings on this site are my own and do not necessarily represent St Catherine's School's positions, strategies, opinions, or policies."

This standard disclaimer does not by itself exempt the St Catherine's School community from personal responsibility when blogging.

Profiles and Identity

Users must remember their association with and responsibility to St Catherine's School in online social environments. If you identify yourself online as a member of the St Catherine's School Community, ensure your profile and related content is consistent with how you wish to represent yourself in person.

Care should be taken when using last names, school names, addresses or phone numbers that appear online.

Users should, when uploading digital pictures or avatars that represent themselves, be sure to select an appropriate image. They should also remember not to use copyrighted images.

Part 3 – Security & Passwords

All users of digital technology at St Catherine's School have an obligation to ensure that any confidential School information is safeguarded. Remote access to the school network necessitates that all mobile devices, which are configured with the School accounts, should be secured with a passcode which should never be disclosed to others under any circumstances.

Strong passwords are a vital aspect of computer security in particular with regard to remote access to the School system.

All users are responsible for taking the following steps.

All staff school network passwords are set to expire every 90 days. It is also recommended that users change their passwords before the end of each term to ensure access is not disabled over holiday periods.

5

Student school network passwords are set to expire once per year.

Staff and students are not required to change their Google password periodically, but must obey password standards of length and complexity in accordance with online accounts.

- Each time you change the password you must use a different unique password
- Passwords must be a minimum of eight characters long
- Take care that they are not observed when typing in passwords
- Passwords should never be written down
- When you change your password on a School personal computer please be aware that your password will also need updating on your mobile devices.

Password Guidelines
A weak password:
- Contains your user name, real name, or company/school name
- Contains a complete dictionary word. For example, Password is a weak password.

A strong password:
- Is at least eight characters long
- Is significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3 ...) are not strong.
- Contains characters from each of the following four groups:
  - Uppercase letters - A, B, C …
  - Lowercase letters - a, b, c …
  - Numerals - 0, 1,2, 3, 4, 5, 6, 7, 8, 9
  - Symbols - ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /

To make your password more secure some examples might be to:
- Put your password in inverted commas
- Add a memorable date at the end
- Start or finish with a capital letter

Part 4 -Health and Safety Guidelines
Where possible all users of computers should check and adjust:

Monitors: The screen should be positioned at arm's length and adjusted for height so that the user has direct vision of the centre of the screen.

Seating: The height needs to be adjusted so that the user's hips are positioned slightly higher than her/his knees. This helps circulation. Users' feet should be either flat on the floor or on a footrest.

The mouse and keyboard: Position these comfortably close to avoid any unnecessary stretching of the shoulders and upper back.

The Health and Safety Executive guidelines on holding a mouse are:
- Position the mouse within easy reach so it can be used with the wrist straight
- Sit upright and close to the desk so you don't have to work with your mouse arm stretched
- Move the keyboard out of the way if it is not being used.
- Support your forearm on the desk and don't grip the mouse too tightly.
- Rest your fingers on the buttons and do not press them too hard.

All users are strongly recommended to take regular breaks, preferably away from the computer desk, at least once every twenty minutes and do some simple stretching exercises to relieve the muscles they have been using, for example hands, wrists and neck. Eye muscles should be refreshed by looking at distant objects as well as those close up.

6

The school iPad classroom guidelines state that break and lunch times should be screen free, to avoid eye strain when using mobile devices. For further information, staff and students should refer to Classroom Guidelines for the Use of iPads.

Part 5 - Guidance for Parents

Parents should consider the following points which indicate how the internet can be made a safer place for children.

We strongly recommend that parents:

- Monitor their own daughter's use of the internet and discuss with her its negative aspects.   The School cannot supervise the use of modern technologies outside School and we depend upon parents' support in this area. Our ICT Department has produced an advice bulletin to protect girls' security on the computer which is on the community area of the school website.
- Monitor their child's internet use; put her computer in a room used by the whole family so that you can see the sites she is logged on to.
- Ask your daughter to show you her Facebook or other social media accounts from time to time, commending what is interesting but also challenging what you may feel to be inappropriate, making her see things as outsiders might see them, e.g. photographs of herself and friends etc. Please note that Facebook regulations are such that accounts are limited to users aged 13 years and over.
- Encourage your daughter to share the internet with you; ask her what sites she is visiting and why she likes them.
- Log on to the sites yourself so you can see what she is using and how the sites work.
- Create a list of internet house rules as a family. This can include sites that are off limits and how many hours can be spent online.
- Tell their daughters never to give out any personal information to people they do not know.
- We recommend that mobile devices are configured appropriately for your daughter's age. For example, restrictions can be set to prevent apps only suitable for adults being downloaded. Consult your provider for guidance.

The community part of the website and parent iTunes U course have a number of links and advice for parents on e-safety. In addition, regular opportunities are provided in school for parents to attend talks and training about online safety and awareness.

Part 6 - Guidance for Students

Advice for the Safe & Correct Use of the Internet & Digital technology by students:

- Use caution when giving out a mobile phone number.
- Ensure your mobile phone has your ICE (In Case of Emergency) numbers of your close family/next of kin programmed into it in line with emergency services requests to help them and hospital personnel in any emergency that rendered you unable to give information in person.
- Never return any communication from an unknown source
- Think carefully about what you read on the internet; question if it is from a reliable source
- Never agree to meet anyone online unless you have permission from your parents
- Remember that many people in chat rooms and on social networks are not whom they say they are.
- Use caution when posting personal information on the internet such as your real name, address, phone number, email address, school, and postcode. Photos of you in your school uniform could be used to trace your location.
- Be careful about putting photos of yourself or friends on websites. Never send photos to someone you have met online.
- Avoid webcam chats with people you do not know.
- Do not respond to emails from people you do not know.
- Learn how to block people on email or websites. If someone sends you inappropriate mail, block them.
- Should you receive any unpleasant material or messages do not respond. Do not be afraid to ask for help from a parent or member of staff.

Adhering to all these basic principles and rules will ensure that ICT devices are used to enhance educational experiences and communication between students and teachers. The internet facilitates learning when harnessed in a safe, informed way by all members of the School Community and the School's ICT systems can be used and kept secure by everyone.

All staff, students and parents are issued with an ICT Agreement which they are asked to sign acknowledging their understanding and agreement to the Guidelines for the use of Digital Technology. This agreement will be reviewed annually and any amendments/additions will require this agreement to be re-signed.

This policy is devised and reviewed by members of the ICT Development Committee and approved by the whole group before publication will be reviewed annually.

Signature of Preparatory School Headmistress: …………………………………

Date…………………………….

Signature of Senior School Headmistress: ………………………………….

Date…………………………….

Signature of Director of Digital Technologies: …………………………………

Date: ………………………………………

Appendices
St Catherine's School Student and Parent ICT Agreement
St Catherine's School Staff ICT Agreement