Charitable Objects of St. Catherine's School *- The Objects for which the Company is established are to promote and provide for the advancement of education by providing, conducting, governing, carrying on and maintaining in the United Kingdom, or elsewhere, a boarding or day school or schools for girls in which the teaching shall be in accordance with the principles of the Church of England.*

St Catherine's School, Bramley
WHOLE SCHOOL POLICY
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 was written in 2013 and reviewed in 2016, May 2018, October 2018 and September 2019 taking into account further regulatory changes. This policy has been developed with reference to and in line with the Education Act 2011, The Use of Social Media for Online Radicalisation 2015, KCSIE (DfE September2018), Preventing and Tackling Bullying (DfE 2017), Sexting in Schools and Colleges: responding to incidents and safeguarding young people (UKCCIS, Jan 2017), ICO General Data Protection Regulation (GDPR 2018)

It should be read in conjunction with the following:
Child Protection Policy
Anti-bullying and Anti-bullying in the Workplace Policies
Code of Conduct for Staff
Confidentiality and Privacy Policy
ICT Policy Appendix 1 - Student Code of Conduct and Student & Parent ICT Agreement
ICT Policy Appendix 2 - Staff Email Charter & Staff ICT Agreement

This Policy, while including essential information about ICT at St. Catherine's is also in part a handbook offering very useful guidelines on the proper use of IT, setting of reliable passwords, use of social media etc. It is essential reading for staff, students and parents.

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 have embraced tablet technology that is revolutionising the way education is delivered around the world. We are proud to be at the forefront of this transformation and have been an iPad School since September 2014.

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 mobile devices and e-safety 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. Parents are always welcome to contact the Director of Digital Technologies directly on: dan.raymond@stcatherines.info

Aim of the Policy: 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 twice-termly basis. This is a cross-phase group with both Headmistresses, academic and ICT staff from both Schools in attendance, a member of the administrative staff, and a School Governor. When necessary, senior pastoral staff are invited to attend when pupil welfare and online safety are discussed. Other staff are invited if a particular area of expertise is required in key discussions. The ICT Development Committee reviews these aims from time to time when its work introduces new elements of ICT provision.

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, keeping the governor representative fully informed of any actions in this area.
- To prioritise appropriately the way in which 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.
- Wherever possible, have regard to minimising environmental impact and the carbon footprint of ICT in both Schools.
- To ensure that the School provides information, guidance and support for parents on the use of personal technology as and when appropriate.

First Published November 2001
Reviewed by the ICT Development Committee November 2018
Previously reviewed by the ICT Development Committee March 2011, May 2015, November 2016

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. School servers are located in a secure physical location with access only by authorized staff
- 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 workstations to provide a comprehensive education in commonly used desktop IT systems.
- Projectors, HD TVs and/or Interactive Whiteboards in a vast majority of classrooms.
- Lockable iPad charging and storage facilities in several locations for day and boarding pupils.
- Apple TVs in teaching and presentation areas for exhibiting content from personal devices.

- The school employs a CCTV system of 35 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.

ICT Key Personnel

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

Name	Position	Responsibility
Dan Raymond	Director of Digital Technology	Overseeing all aspects of the ICT Provision
Matt Coppinger	IT & Anniversary Halls Technician	Support of IT systems and Anniversary Halls
Jack Matthews	IT Technician	Support of IT systems
Matthew Birch	Apprentice IT Technician	Support of IT systems
Katie Malins	Director of Digital learning, Computing and ICT (Prep School)	Computing, ICT and E- Safety (Prep School)
Laura White	Coordinator of Digital Learning	Use of technology for teaching and learning
Davina Byrne	Lead Teacher of Curriculum ICT	Staff Training

Guidelines for the use of Digital Technology Inside & Outside School

Contents

Part 1 –Acceptable Use

Guidance for pupils is delivered 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 takes place internally including PREVENT, and during INSET including use of technology in the classroom.
Parents receive 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. This enables parents to continue with essential work commitments/pressures during gaps between matches or while accompanying their daughters to activities.

Staff, pupils ***and*** parents therefore all sign an IT agreement to acknowledge the principles and terms of responsible conduct regarding technology at St Catherine's.

School Owned Digital Technology

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 on school resources. Storing personal files such as music, digital pictures and video on the School system is not permitted.

School Computers and Internet Access

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 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.
- Pupils should not be using classroom equipment to log on for personal study or use without prior permission of the member of staff and in his/her presence.
- 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.
- The School's own mobile devices e.g. iPads and Laptops are for use in school only; they should only be taken off site with direct permission from the Director of Digital Technologies.
- All new software must be deployed by authorized IT Support staff. Requests by pupils for apps for use on School devices are to be made to the IT Support Department - apps are not to be downloaded onto the School's devices using personal accounts.
- Copyright or licensed software must be used in accordance with the software license.
- School devices are a shared resource and should not be personalised or customised in any way or synced with personal computers or iTunes accounts.
- Any faults or damage to school owned devices must be reported to a member of staff as soon as possible.

Personally Owned Digital Technology

St Catherine's is aware of the benefits of using privately owned devices at school and is mindful that these are expensive and versatile devices and in order for everyone to use them effectively, guidelines must be embraced and upheld by everyone.

The School recognises the empowerment of students to acquire knowledge, learn new skills, research independently and develop their identities using a device that is theirs and one that they are comfortable using. The School will make a best-efforts attempt if technical support is required for any personal device during the school day but cannot guarantee an immediate solution. St Catherine's is proud to be an iPad school and supports the use of Apple iPad for learning, academic and professional purposes. The school's comprehensive mobile device facilities are geared toward Apple devices, but the IT support department is also able to offer advice and help to all staff and students regarding the current mobile technology landscape and the various options therein.

St Catherine's BYOD Policy

Years PP1 - Lower 2
Mobile phones and all other forms of digital technology are only permitted in school with written permission from the Headmistress of the Preparatory School. Kindles and other e-readers are permitted for use by Lower 2 students.

Years Upper 2 – Upper 5
Upper 2 to Upper 5 are required to bring a personal iPad to school to complement their studies. **A laptop or other device substitute is not permitted until the Sixth Form years.** The iPad should be updated with the latest iOS, hold sufficient charge to last the school day, and be in good working order so not to impede use in the classroom. Adequate software upkeep and the ability to install new apps as directed is necessary to reduce the risk of data loss and facilitate access to digital resources as required. At this early stage of school use, Prep pupils' personal iPads are commissioned and managed by the School in partnership with parents. This enables each pupil to have access to the educational apps we recommend which are populated by the School and ensures that girls have

access to similar digital learning experiences. These steps are also are taken to safeguard pupils. The School offers the option to purchase iPads via school at an educational discount.

Prep School
Fitbits, smart watches and other digital wearable technologies are not permitted in the Prep School.

Sixth Form
Girls in the sixth form may use any laptop or tablet device in their studies, as appropriate within the IT Policy. A mobile device such as an iPad continues to be beneficial but is not mandatory. Personal laptops are permitted and recommended, in preparation for Further and/or Higher Education.

The current minimum requirements for an iPad to be used at school are:

- Screen size of 9.7" or larger. An iPad mini is not recommended for school.
- Storage capacity of 64GB or greater
- Functioning battery life of 6+ hours to last the school day
- Visibly good condition
- An iPad should typically last three years, requiring a single replacement approximately halfway through the Senior School.
- For students in the Senior School who definitely wish to use a physical keyboard, we encourage that it be a removeable, wireless keyboard which resides at home.
- An Apple Pencil is not mandatory at present, and those who choose to use one must take care to mark it carefully as theirs and to have a note of its serial number. These pencils are easily mislaid and identical. Proof of ownership is almost impossible without labelling.

The school operates an iPad purchasing portal in the Summer term each year, through which we are proud to pass on our educational discount and a generous insurance option to parents. A ClarionCall will be sent each year with advice relevant to the current models, inviting orders to be placed on the school website during term time for collection at the end of the school year.

All mobile devices brought into school should be insured. St Catherine's accepts no responsibility for any damage or loss. Mobile devices should be named and protected by a suitable case.

Pupils should keep their device protected from damage when not in use, either in their bag, personal locker or the lockable charging facilities. In the iPad years, an iPad is necessary for studies and any damage or degraded usability must be repaired promptly. The IT Support department can make short term loans from school stock while a personal iPad is undergoing warranty repair or replacement.

All students/parents are responsible for purchasing and installing antivirus and anti-spyware software on personal laptops and keeping this up to date where applicable. Free versions of popular antivirus solutions such as AVG and Avira are quite adequate when coupled with responsible use of the Internet.

If the device has standalone Internet capability (e.g. 3G/4G), the school cannot take any responsibility for internet use; therefore we ask parents to provide non-enabled or data-blocked devices which can only access the Internet via the School's Wi-Fi system, which includes a filtering and monitoring system.

Smart watches of any kind that link to Wi-fi are not allowed in years U3 to U5.

FAQ: Do pupils need to use an Apple MacBook in 6th Form?
An Apple MacBook is not ***necessary*** to access school resources but is often preferred by students for ease of use, reliability and longevity. In most cases the same device will also serve well at university and this is an appealing option. We would advise not discarding the iPad completely. It has its specific functions that a Laptop does not have.

FAQ: Why are pupils below the Sixth Form not allowed to use a laptop in class?
This is because they are tempted to touch type notes verbatim which is poor training for notetaking. The wall of screens between pupils and staff impairs communication. The iPad is much more flexible as a learning tool, being

able to take photographs and film, run a wider variety of specific apps, and maintain speed and reliability over many years. It is also less cumbersome in a rucksack of many books/files etc. At Sixth Form level, girls are carrying fewer devices, are older and more used to the sophisticated Microsoft programmes which they use to present academic work and more likely to select a MacBook or PC alternative, or to complement their iPad.

FAQ: Do parents need to buy any software?
No. All students are able to download the Microsoft Office package free of charge via The School's Office 365 subscription. Many Windows software items are accessible via the school's Remote Desktop facility. All commercial iPad apps are gifted to students by the school.
Some software pertaining to specific subjects, may only be installed in designated IT rooms or departmental computer suites, and can only be used in those areas.

Part 2 – Security & Passwords

Profiles and Accounts

Staff and pupils from PP3 upwards are provided with ownership of a unique username and password combination. They are given access to a personal documents area and granularly-permissioned communal shared areas. All account security events are logged.

As part of St Catherine's Digital Learning programme, we also provide the opportunity to access our online educational domains as well as our internal school network. St Catherine's uses both common educational providers, Google and Microsoft, to provide a gamut of learning tools, opportunities and benefits.

Google 'G Suite' and Microsoft 'Office 365' are diverse collections of online tools for storage, collaboration, document creation and editing which can be accessed from staff or girls' iPads or any computer. They are also used to synchronise information between school and personal devices, and sign into additional education websites without a surplus of additional usernames and passwords.

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 and will not bring the school into disrepute.

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.

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 any mobile devices that are configured with the School accounts should be secured with a passcode which should never be disclosed to others under any circumstances.

St Catherine's Network Passwords Summary

Students and staff are regularly advised and reminded of the need to manage their password by training from ICT teachers, automatically generated e-mails and direct communication from the IT Support department.

The below table summarises the password policy enforcement for staff, students and guest accounts. This strategy is in support of SSO (single sign on) to online providers used by the school such as Office 365 and G Suite for Education. In all cases, staff and students are required to respect password privacy and model good practice.

User Account	Categorisation	Password Criteria	Details
Staff	Password Policy Enforcement: High	8+ characters Complex password 90-day expiration	This includes all teaching & support staff including Governors, supply/assistant teachers, IT support, staff helpers and auditors/inspectors.
Senior School Students	Password Policy Enforcement: Medium	8+ characters Complex password	Students conform to the same high standards of password complexity and independence as staff.

		375-day expiration	
Prep School Students (U2 & L3)	Password Policy Enforcement: Medium	8+ characters Complex password 375-day expiration	Students in U2 and L3 use a complex assisted personal password with teacher oversight e.g. "Potato4680".
Prep School Students (F1 & L2)	Password Policy Enforcement: Low	8+ characters Optional Complexity No expiration	Students in F1 and L2 begin to take ownership of an enhanced alphanumeric password.
Prep School Students (PP1 – PP3)	Password Policy Enforcement: Low	8+ characters Optional Complexity No expiration	Students in Pre-Prep do not use passwords. Computer use is chaperoned and supervised by a teacher at all times.
Shared or Guest Accounts	Discretionary Policy Enforcement	6+ chars Optional Complexity no expiration	Low risk accounts used for guest, presentation, exam, or network purposes. Typically, low access or short-term accounts such as Parents, Lets & Events

Passwords are stored with non-reversible encryption by The School and are not retrievable or accessible by the IT Support department. The user account and content within remains the property of the school, and if intervention or help is required, the password will be reset.

All users are responsible for the safekeeping of their school credentials. Access to the system must only be made with the user's own account and password, which must not be given to any other person except where expressly permitted by the Director of Digital Technologies.

For special cases, many more factors are present as well as password strength and complexity. The Director of Digital Technologies and Director of Staff (Senior School) or Deputy Head, Staff (Prep School) will make assessment of appropriate password criteria taking into account the risks, timeframes, benefits and accessibility requirements of the situation.

St Catherine's Complex Password Guidelines

The popular definition of a complex password and the requirements are:

- may not contain any of your names or your username
- a minimum of eight characters, and containing characters from at least three of the following groups:
    - Uppercase letters - A, B, C …
    - Lowercase letters - a, b, c …
    - Numerals - 0, 1,2, 3, 4, 5, 6, 7, 8, 9
    - Symbols - ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /

St Catherine's complex passwords are automatically rejected if they do not meet these criteria. They are subsequently replicated to online accounts and are changed with greater frequency than usually required by most websites, upholding a better-than-average standard of online security.

Creating a Strong Password

A strong password is one that is easy for you to remember but difficult to crack by automated guesswork or discern from a previous version of the password. To make your password more secure, some suggestions are:

- Compact a memorable sentence into a word. For example, "I have a rabbit called Dennis who eats Carrots." becomes "IharcDweC."
- Add a memorable date or string of numbers to your favourite word.
  You should not use your birthday, PIN or telephone number in any password
- Start or finish with a capital letter or punctuation symbol.
- Invent and follow a convention to cater for regular password changes. Note that this must ensure a more significant change with each version than merely incrementing numbers.

Avoid things which may cause your password to become weak or problematic:

- Avoid complete standalone dictionary words. For example, *Password* is a weak password.
- Your password should be significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3 ...) are not strong.
- Avoid symbols # or @ or " which may not appear reliably on all keyboards.

- Do not reuse the same password for many different types of service, as this will swiftly degrade the security and usefulness of even the best-chosen password.
- Do not reveal your password to anyone unless by agreement with the School.
- Do not write down your password, but you may use approved methods to record passwords as part of a secure solution. See below or if in doubt, contact the IT Support department.

Passwords of staff and students from U2-U6 are synchronised to their online Google and Microsoft accounts, and adhere to the password requirements of those services. When you change your school password, please be aware that your password will also need updating on your devices for those online services.

Online Passwords Guidelines

Passwords for websites and online accounts are numerous and vary greatly in levels of risk and consequence. An ongoing strategy is advisable according to the nature and quantity of passwords involved.

1. For websites which hold a functioning email account or significant personal data/tracking, such as Apple, Google, Microsoft, Yahoo, Dropbox, Facebook, it is advisable to use a strong, complex password which is unique to that website.
2. For websites which hold data about you, such as your real name or address, commit a strong, complex password to memory, or adopt a password convention.
3. For common and inconsequential websites that hold no data about you (not even your name) and represent an insignificant risk if they were compromised or hijacked, you may nominate an expendable password. You can use this same password across similar expendable websites without raising your risk profile.

Strategies for Managing Passwords and 2-factor Authentication

- You may leave an unlabelled hint to your password (for example, the numerical component disguised as a phone number, or the complete version of a compacted sentence) in a private location.
  This can serve as a discrete reminder but should not make your password obvious to anyone.
- Formulating a convention for website passwords should be a personal invention. One example is to take the first and last letter of the website and add a memorable sequence of numbers and letters in between. This will not make other passwords obvious if a single website is compromised and your credentials are stolen.
- Only the use of password management repositories, tools and software which have been approved by the IT Support department, are permitted. Password management software involves a master password, which must have the same or better security and exclusivity, than any of the passwords being protected.
  - The password management of modern browsers such as Safari and Chrome allow passwords to be saved and auto-filled with great convenience across all devices.
  - Online, reputable password management software such as those from https://www.lastpass.com/ or https://www.dashlane.com/ are functional repositories, albeit with premium limitations.
  - A free, encrypted offline reference for passwords can be downloaded from https://keepass.info/.
- Note that 2-factor authentication or 2-step verification is a gold standard of security which should be aspired to for critical online accounts such as those with access to your finances. It is encouraged and supported by training from the IT Support department but is not mandatory for school services.

Part 3 – Internet Use

Internet access for all purposes is reviewed regularly by the IT Support department and the ICT Development Committee. 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 or potentially distressing material, the school additionally monitors and reports on related online activity. The level of monitoring and filtering is under constant review.

Access to the Internet is filtered and monitored by the school firewall. The school has primary and backup ethernet & fibre connectivity and receives daily updates regarding URL categorisations from specialised online services. Uncategorised websites are blocked but may be requested via the IT Support department.

Internet Filtering

The firewall provides year-group-based internet filtering and special permissions as required by the school. The firewall delivers reports on activity for all users of the school internet, collectively or individually. Curfews are implemented for the boarders as stated below:

Year Group	Total Internet Availability	Social Networks	Gaming
Upper 6	06:00-23:59	during internet hours	during internet hours
Lower 6	06:00-23:59	during internet hours	during internet hours
Upper 5	06:30-22:45	06:30-07:30 weekdays 20:30-22:45 weekdays weekends	06:30-07:30 weekdays 17:30 to 19:00 weekdays 20:30-22:45 weekdays weekends
Lower 5	06:30-22:30	06:30-07:30 weekdays 20:30-22:30 weekdays weekends	06:30-07:30 weekdays 17:30 to 19:00 weekdays 20:30-22:30 weekdays weekends
Upper 4	06:30-21:30	06:30-07:30 weekdays 20:30-21:30 weekdays weekends	06:30-07:30 weekdays 17:30 to 19:00 weekdays 20:30-22:30 weekdays weekends
Lower 4	06:30-21:30	Blocked	06:30-07:30 weekdays 20:30-21:30 weekdays weekends
Upper 3	06:30-21:30	Blocked	06:30-07:30 weekdays 20:30-21:30 weekdays weekends

The following are examples of blocked categories: Proxy Avoidance, Gambling, Nudity, Spam, Drugs, Dating, Illegal, Radicalisation, Weapons, Hate, Racism, Violence.

Websites and services are reviewed individually from permitted categories such as social media, entertainment, streaming media and instant messaging. Disreputable or compulsive services such as Snapchat and Netflix are carefully reviewed, and additional controls may be imposed at any time.

All users of the school network must adhere to internet controls in place and no attempts to bypass them are permitted. Girls are forbidden to have a Virtual Private Network (VPN) of any kind on their devices during term, even if they have used these with parental knowledge and permission while travelling abroad in the holidays. For their own safeguarding, their devices must be within the protection of the school's controls.

In the event of accidental breach, please seek the immediate guidance and support of the ICT support department.

Mobile Data

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, Instagram, WhatsApp, Snapchat and Twitter, as well as to more general types of social media and instant messaging 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 even your earliest posts on social media. 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 feature a student's full name.
- 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 on social media between current or recently departed students 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.

Part 4 - 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. They must use this to communicate with each other and make no use of personal email addresses for school business. Safeguarding regulations preclude staff from contacting girls by any other address.

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.

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.

Staff should follow the advice outlined in the St Catherine's Staff E-mail Charter.
Parents are invited to email staff with queries or concerns but we respectfully ask that an answer is not expected between the hours of 6 pm and 8 am

Part 5 - Printing

St Catherine's is an 'eco-school'. As such, we believe in the 'green' use of IT and feel strongly that any member of the school should only print if absolutely necessary. ***'Think before you print!'***

The School uses PaperCut print management software. Each member of staff and each Senior School student is provided with a PaperCut number. This enables the release and auditing of print jobs when he or she is in proximity to Papercut-enabled photocopiers and printers. School printers are configured to print in greyscale as part of our eco initiatives.
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.

Part 6 - 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.

The devices of 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.

Part 7 - Remote Access

St Catherine's School staff and students from Upper 4 to Upper 6 have the facility to access the School network resources whilst away from school via our Remote Desktop facility. Staff and students are required to be vigilant when accessing systems remotely. Computers or other digital devices should not be left unattended when connected.

1. Remote users will be disconnected if left unattended for an extended period of time.
2. Remote users need to pass additional security checks i.e. re-entry of their school password, and knowledge of the current door code
3. Remote users must make sure they are not being overlooked by anyone, even family, when accessing confidential data.
4. Network access should not be shared with friends or family members, and they should not use the School system.

Part 8 - 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.
Mouse, keyboard and touchpads: Position these comfortably close to avoid any unnecessary stretching of the shoulders and upper back. In all cases the wrist should be comfortable and with adequate lift to reduce the common risk of repetitive strain injury. The mouse should be within easy reach and in an uncluttered area of desk, with adequate traction and support for forearm and wrist.

Mobile devices: No device should be used while walking in school, and care should be taken not to use heavier mobile devices such as tablets in an unsupported way for extended periods of time.

All users are strongly recommended to take regular breaks, preferably away from the computer desk and screens, at least once every thirty 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.

Having read this Policy with care, staff, girls and students are required to sign the agreement in Appendix 1 for parents and students, and Appendix 2 for staff and return it to School. Parents are asked to check that their daughters have understood the policy and any other family policies in place at home – hours of use, other monitoring software etc. Parents of boarders are asked to do this during a holiday but can rest assured that boarding housemistresses can answer any queries the girls may have.

ICT Agreement

All staff, students and parents are asked to sign this agreement, acknowledging their understanding of, and agreement with, the Guidelines for the use of Digital Technology.

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

This Agreement will therefore also be reviewed and from time to time be presented to be re-signed when significant developments occur in the School's ICT provision for staff, girls or parents which will be reflected in the Policy.

Signature of Headmistress: …….

Date…….

Signature of Preparatory School Headmistress: …….

Date…….

Signature of Director of Digital Technologies: …….

Date…….

Appendices

ICT Policy Appendix 1 - Student Code of Conduct and Student & Parent ICT Agreement
ICT Policy Appendix 2 - Staff Email Charter & Staff ICT Agreement