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 BRAMLEY

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

'Believe… Achieve… Succeed'

Policy Holder	**Dan Raymond**
Date Approved	**September 2025**
Approval	**ICT Development Committee**
Date for next review	**September 2026**

Aims of the Policy

This policy is written to:

- promote the successful use of digital technology and to enhance teaching and learning at all levels.
- keep children safe from online threats and exposure to inappropriate, extremist or potentially distressing material.
- To support parents in managing their daughter(s) use of personal devices.

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, Preventing and Tackling Bullying (DfE 2017), ICO General Data Protection Regulation (GDPR 2018), 'Sharing nudes and semi-nudes: how to respond to an incident' Updated March 2024 (UKCIS), KCSIE (DfE September2025), JCQ regulations (sections 3.20 and 3.21 of the *General Regulations for Approved Centres*)

It should be read in conjunction with the following School Policies:

- Safeguarding and Child Protection Policy
- Anti-bullying and Anti-bullying in the Workplace Policies
- Code of Conduct for Staff (Staff only)
- Confidentiality and Privacy Policy
- ICT Policy Appendix 1 - Student and Parent ICT Agreement

Scope of the Policy

This policy applies to all staff, students, governors, and any additional individuals who have access to St Catherine's IT systems and data.

Key Roles and Responsibilities

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

Name	Position	Responsibility
Denise Irons	Deputy Head, Staff, Prep School Deputy Designated Safeguarding Lead	Online safety monitoring (Whole School)
Matthew Parry	Deputy Head, Curriculum Prep School	Online safety monitoring (Prep School)
Dan Raymond	Director of Digital Technology	Overseeing all aspects of the ICT Provision Online safety monitoring (Whole School)
Matt Coppinger	IT Manager	Support of IT systems and cyber security. Support of Anniversary Halls
Matthew Birch	Senior IT Technician & App Developer	Support of IT helpdesk. Development of school apps
Sandip Gurung	IT Technician	Supporting all colleagues and students with IT systems.
Katie Malins	Director of Digital Learning, Computing, and ICT (Prep School)	Computing, ICT, and online safety monitoring (Prep School)
Angelique Burns	Coordinator of Digital Learning	Use of technology for teaching and learning
Davina Byrne	Lead Teacher of Curriculum ICT E-Safety Coordinator	Staff training Online safety monitoring (Senior School)
Vic Alexander	Deputy Designated Safeguarding Lead	Online safety monitoring (Senior School)

ICT Development Committee

The strategic 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 Heads, a Deputy DSL, academic and ICT staff from both Schools in attendance, a member of the administrative staff, and a School Governor. When necessary, senior pastoral staff/other DDSLs 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 its specific aims from time to time when its work introduces new elements of ICT provision.

Part 1 – Responsible Use

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

Personal Responsibility

Online behaviour should reflect the same standards of honesty, respect, and consideration that is expected with in-person interactions.

Users are personally responsible for the content they publish online. When contributing online, do not post confidential or personally identifying information such as last names, school names, addresses or phone numbers.

Publishing any material that defames the school will be dealt with as a serious disciplinary matter. Users must remember their association with and responsibility to St Catherine's School in online social

environments. 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."

The above disclaimer does not by itself exempt the user from personal responsibility.

- Before posting photographs and videos, permission should be sought from the subject where possible and thought given to the question of whether the image is appropriate.
- Staff posting photographs of girls on any online channel 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 on the public section of the school website will feature a student's full name.
- No student should save or proliferate photographs of a member of staff.
- Personal connections on social media between current or recently departed students and staff social media accounts are not allowed. Communication via social media is overseen by the Director of Digital Technologies, the Senior Housemistress and the Marketing Department.

All users of digital technology at St Catherine's School have an obligation to ensure that any confidential School information is protected, pupils are safeguarded, and the principles of this policy are upheld at every opportunity.

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.

- 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.
- Any devices configured with a St Catherine's account should be secured with a passcode which should never be disclosed to others under any circumstances.
- Computers and associated equipment must not be tampered with in any way. Pupils should not use classroom equipment 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.
- USB storage devices are not permitted in the normal use of IT at school unless authorised by the Director of Digital Technologies.
- The School's centrally stored 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 authorised IT Support staff. Requests by pupils for apps for use on School devices are to be made to the IT Support Department.
- 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 online accounts.
- Any faults or damage to school owned devices must be reported to a member of staff as soon as possible.
- 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.

Personally Owned Digital Technology

The use of privately owned devices is outlined in the St Catherine's Device Policy. For everyone to use personal devices effectively, guidelines must be embraced and upheld by everyone.

- All personally owned 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.
- All staff, parents and students are responsible for maintaining security updates, and complying with the manufacturer's operating system update schedule, on devices which will connect to the school network
- 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.
- When girls are provided with 3G/4G/5G enabled devices - phones in particular - the School cannot guarantee protection from inappropriate websites.
    - Parents should ensure that the provider has enabled controls to block access to 18+ rated content via the mobile Internet service
    - We advise parents not to provide unlimited data to students thus ensuring that most access is via controlled Wi-Fi at home or in school.
    - The ideal solution is a non-enabled or data-blocked personal device which can only access the Internet via the School's Wi-Fi system, which includes a filtering and monitoring system.
- The school reserves the right to make checks of students' devices if there is a reasonable suspicion of harm or intended harm affiliated with the device. This is to ensure that students are learning and practising positive communication and not being tempted into the use of inappropriate language or unkindness online. This is part of the students' education and the School's control and intervention strategy which we anticipate parents will be enforcing at home, complementary to school.

St Catherine's Device Policy

Years PP1- Lower 2

Pupils have access to shared banks of iPads and our computer suite for specific lessons under the direction of their teacher. Limited devices or special configurations of tablet computers are permitted for use by Lower 2 students with agreement from their Form Teacher.

Years Upper 2 - Lower 3

The School provides a school iPad with a protective case and 24/7 Internet filtering and monitoring, repurposed for this age group. A modest termly charge is made to parents for this, covering the rental of the device, associated services and the full cost of repair or partial cost of replacement if the iPad or accessories are lost or damaged. The school will enact all repairs through an approved and trusted provider. Girls will return the iPad to us when they leave the Prep School.

Years Upper 3 – Upper 4

The School deploys a new iPad with a suitable protective case, stylus and insurance package in a financial agreement of nine termly payments starting from the beginning of Upper 3. The School commissions, manages and deploys the iPads with all educational apps for an optimal digital learning experience.

Years Lower 5 – Upper 5

Lower 5 to Upper 5 may either continue to use the previous iPad or acquire a new managed device service from the School. *A private laptop or other device is not permitted until the Sixth Form years*. All iPads should be updated with the latest iOS, hold sufficient charge to last the school day, and be in good working order so as not to impede use in the classroom.

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, but they should retain the functionality for digital inking which is an essential mode of curriculum resource delivery.

Mobile Phones

For students from Upper 3 to Upper 5, phone use is restricted during the school day. Upper 3 to Upper 4 students are required to lock their phones in a Yondr pouch at the start of the school day and unlock at the end of the day. Lower 5 and Upper 5 students must keep their phones out of sight and out of use throughout the school day.

Sixth Form students should keep phone use to The 6 Boarding house and other Sixth Form spaces. Sanctions will apply for students who do not comply.

Smart Accessories

Smart watches and other interactive wearable technologies are not permitted in school. Other devices including passive trackers such as Fitbits, are not permitted in the Prep School or in any exam areas in the Senior School.

Pupils should keep their school-issued device protected from damage when not in use, either in their desk (Prep School), rucksack/bag, sports locker. The IT Support department can make short term loans from school stock while a device is undergoing warranty repair or replacement.

From Upper 2, we recommend that a pair of headphones are brought to school for flexible study, independent learning and video conferencing and streaming. These should be suitable for use with their primary learning device.

Part 2 – Cyber Security

Technical Security Measures

St Catherine's implements the following security measures:

- Firewalls and network security controls blocking access to malicious or dangerous websites.
- A robust, enforced password policy for all online accounts.
- VLAN separation of school-issued devices and personal/visitor/guest devices.
- Software updates on all devices for security updates and anti-malware definition updates.
- Regular operating system software updates and device/patch management.
- Secure data backup and annual tested recovery procedures.
- Encryption for outbound sensitive and personal data sent to authorised data processors.

- Multi-factor authentication (MFA) for remote access to critical systems.
- Secure configuration of cloud environments (Microsoft 365, Google Workspace).
- Proactive monitoring and alerting solution for security events in Microsoft 365 cloud.
- Prompt removal or reduction of access for leavers' accounts.

User Accounts and Passwords

Access control and permissions are based on job roles and reviewed regularly. The creation and deletion of accounts are monitored by the IT Support department.

Students and staff receive guidance on password management from the IT Support department, ICT teachers, and automatically generated e-mails.

- Student passwords must be at least 10 characters and staff passwords must be at least 15, consistent with modern cyber security principles which prefer length to traditional "complexity".
- A typical school password will consist of at least 3 words separated by spaces or special characters.
- New passwords are randomised to a suitable "strength" and supplied ready to use immediately.
- 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. If it is believed that a password may have been exposed/become known to others, staff will inform their senior leader/line manager immediately
- Exposed passwords will be changed as soon as possible
- Passwords will typically last up to two years before an automatic renewal/expiration notification.
- Re-using passwords from elsewhere for access to St Catherine's systems is not permitted.
- Passwords are stored with non-reversible encryption by The School and are not retrievable or accessible by the IT Support department.
- Modern browsers such as Edge, Safari and Chrome are authorised for the management of passwords to be saved with the support of MFA and biometric identification on those devices.
- For special cases such as temporary access to a singular resource, the Director of Digital Technologies and Director of Staff (Senior School) or Deputy Head, Staff (Prep School) will make assessment of appropriate password criteria, considering the risks, timeframes, benefits and accessibility requirements of the situation.

Staff Training and Awareness

All staff undergo cyber security training appropriate to their role. Best practice, advice and guidance is delivered via staff INSET training for all IT systems, particularly those where learner information, learner work or assessment records are held.

- Staff who have access to awarding bodies' online systems undertake annual cyber security training to comply with JCQ regulations, such as:
    - Creating a strong, unique password
    - Keeping all account details secret
    - Enabling additional security settings wherever possible
    - Updating any passwords that may have been exposed
    - Setting up secure account recovery options
    - Reviewing and managing connected applications
    - Recognising all types of social engineering/phishing attempts
    - Monitoring accounts and reviewing account access regularly
- Phishing security tests and associated awareness and defence training is conducted annually for all staff and students.

Staff training in safeguarding takes place internally including KCSIE and PREVENT, and during INSET, including use of technology in the classroom. Records of training are retained for all staff.

Incident Response Plan

All staff members must report any suspected security incidents or concerns to the IT Support Department immediately, as well as the relevant awarding body, the ICO, NCSC or other organisations where relevant.

Concerns can be reported by email. In the event of a serious concern regarding current activity or a breach, staff should utilise Teams or the emergency mobile contact telephone number for an immediate response.

The Director of Digital Technologies will coordinate the incident response for breaches of cybersecurity and data protection and enact the communication plan for stakeholders.

The Director of Digital Technologies will conduct a post-incident review process to identify lessons learned and update procedures if necessary.

Part 3 – Internet Use

Internet access for all purposes is reviewed regularly by the IT Support department and the ICT Development Committee. The School monitors the use of its computer systems, including:

- the monitoring of web browsing activity and online app behaviour
- document/images/videos created or stored via school accounts
- e-mails and communications sent via school accounts or using school facilities

Internet Filtering and Monitoring

- 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.
    - Filtering provides content control – blocking or allowing content using USLs, keywords, content categories. It helps protect users from potential harm, minimises distractions from learning, but is balanced between protection and over-blocking. Filtering is appropriate to the age, developmental stage and understanding of pupils.
    - Monitoring is the supervision (physically or via technology) of what pupils are accessing. It provides protection from online bullying, verifies learners are acting responsibly and learning acceptable online behaviour, ensures the filtering system is working well and provides a safe place to learn from mistakes.
- 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. The following are examples of blocked categories: Proxy Avoidance, Gambling, Nudity, Spam, Drugs, Dating, Illegal, Radicalisation, Weapons, Hate, Racism, Violence. Curfews are implemented for the boarders regarding access to social networks and gaming websites.
- 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 online safety breach, staff and students should seek the immediate guidance and support of the ICT support department.

Artificial Intelligence

The educational community has a duty to respond to the progression of powerful technologies such as Language Learning Models and Generative AI. Across our curriculum we continue to show students how to use AI beneficially and how to reference it but also pointing out when use is not appropriate or counter productive. All students should be in the position to be able to use AI with confidence and be aware both of its shortcomings and the need to uphold academic integrity. We ensure that we give as much opportunity as possible for higher-order, independent thinking that responds to the specific material covered in lessons. Contextualisation of work ensures that students develop a clear understanding and learn with confidence, even when conducting research that may involve assistance from AI. We will continue to learn and adapt to the latest emerging technologies for maximum benefit to girls' education.

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 from Form I upwards 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 Head.

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.

Parents are invited to email staff with queries or concerns, but we respectfully ask that an answer is not expected between the hours of 6pm and 8am

Students also have access to the "Whisper" platform for anonymously contacting school with concerns or questions, where they do not feel comfortable communicating via other channels.

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 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 - 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.

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

Part 7 - 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.
- **Regular Breaks:** 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 for a short time.

Agreement of the Policy

Having read this Policy with care, staff, girls and parents 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 discuss the policy closely with their daughters and check that they 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.