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

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

GUIDELINES FOR THE USE OF DIGITAL TECHNOLOGY

'Believe… Achieve… Succeed'

Policy Holder	Dan Raymond
Date Approved	September 2026
Approval	IT Strategy Group
Date for next review	September 2027

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
- Staff Code of Conduct
- Confidentiality and Privacy Policy
- Mobile Phone and Personal Devices Policy
- ICT Policy Appendix 1 - Student and Parent ICT Agreement

Scope of the Policy

This policy applies to all staff, pupils, governors, and any additional individuals who have access to St Catherine School'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	Prep School Deputy Head, (Pastoral and Wellbeing) and Deputy Designated Safeguarding Lead	Online safety monitoring (Whole School)
Matthew Parry	Prep School Deputy Head (Academic)	Online safety monitoring (Prep School)
Dan Raymond	Director of Digital Technology, Staff Training	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, Staff Training	Support of IT helpdesk. Development of school apps
Sandip Gurung	IT Technician	Supporting all colleagues and pupils 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, Staff Training	Use of technology for teaching and learning
Vic Alexander	Deputy Designated Safeguarding Lead	Online safety monitoring (Senior School)

IT Strategy Group

The strategic management of ICT in the School is undertaken by the IT Strategy Group 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 IT Strategy Group 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 ICT agreement to acknowledge the principles and terms of responsible conduct regarding technology at St Catherine's School.

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 (within the past year) and staff social media accounts are not allowed. Communication via social media is overseen by the Director of Digital Technologies, the Heads of Boarding Houses 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- L2 (Reception – Year 4)

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 L2 pupils with agreement from their Form Teacher.

Years U2 – L3 (Years 5-6)

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 U3 – U4 (Years 7-9)

The School deploys a new Surface Pro with a suitable protective case, stylus and insurance package in a financial agreement of nine termly payments starting from the beginning of U3. The School commissions, manages and deploys the devices with all educational apps for an optimal digital learning experience.

Years L5 – U5 (Years 10-11)

L5 to U5 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 (Years 12-13)

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 pupils from U3 to U5 (Years 7-11), phone use is restricted during the School day so pupils 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.

Sixth Form pupils may only use their phone in The Sixth Form Library (SHLib) and Sixth Form Common Room. Sanctions will apply for students who do not comply.

Personal Devices

Personal devices include smartwatches, personal tablets and any portable electronic or wearable technology with similar functionality to a mobile phone 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 U2 (Year 5), 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 School 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 School 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 Senior School Deputy Head (Academic) or Prep School Deputy Head (Pastoral and Wellbeing) 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 IT Strategy Group. 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. Please refer to the separate School AI Policy for further detail.

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 6.00pm and 8.00am

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 School 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 pupil 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 U4 to U6 (Years 9-13) 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, pupils and parents are required to sign the agreement in Appendix 1 for parents and pupils, and Appendix 2 for staff, and return it to School.

Parents are asked to discuss this 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 Heads of Boarding Houses can answer any queries the girls may have.

APPENDIX 1 – STUDENT AND PARENTS ICT AGREEMENT

This Agreement is an appendix to the 'Whole School ICT Policy - Guidelines for the Use of Digital Technology' which will be reviewed annually and significant amendments/additions to either document will require this Agreement to be re-signed. All new joiner pupils (from Form I) are asked to read and sign it on arrival before accessing any of the School's online services. New joiner parents are also asked to sign that they have read and agreed the policy.

This agreement has been devised to ensure that all students and their parents/carers/guardians are aware of the acceptable use of technologies and the areas which need to be handled with appropriate caution to avoid putting themselves or their friends at risk through careless or thoughtless behaviour. The School supports parents by complementing their monitoring of their daughter(s) use of her digital devices and, like parents, reserves the right to make random checks of any girl's devices in order to ensure consistent standards of proper behaviour/language etc. are maintained online throughout the School.

These rules and guidelines protect students and the School by stating clearly what is acceptable and what is not. They are given to every student to take home to be read, discussed and signed by the girl herself (Form I and above) and her parents, and are returned to the School.

Part 1 – Care of Technology and Data

If a fault arises with personal technology, the School will make a best-effort attempt to provide technical support but cannot guarantee an immediate solution. In the case of school devices which are necessary for studies, the IT Support department can make short term loans from school stock while a personal school device is undergoing repair or replacement. A suitable agreement will be supplied where school devices are loaned or leased by the School, stipulating the conditions of the loan. All school devices are only loaned for educational purposes and are set up to limit apps only to those necessary for schoolwork.

- From U2 (Year 5) when the girls have access to a school-managed iPad, we ask pupils to: Keep their school device clean and presentable – the screen can be cleaned using a soft cloth.
- It is their responsibility to ensure their device is fully charged each day. Mobile devices must be used on battery power as mains sockets may not be suitably positioned within classrooms.
- It is their ongoing responsibility to handle their digital resources safely and keep them organized. Documents should have clear titles, topics and dates as soon as they are created. Printed work should have a name clearly displayed.
- Make sure that all their work is backed up following correct procedures. iCloud backup must be turned on and backing up regularly.
- Ensure that the "Find My" app or an equivalent service is enabled on all devices.
- Ask for help with unresolvable error messages and remove issues with backups, passwords, or storage as soon as possible. The IT support department is available in person or by e-mail for all students.
- At all times, in all communications and in any application use appropriate language and courtesy to any correspondents. This also applies to the use of mobile phones.

Part 2 – Appropriate Use

St Catherine's School is committed to the use of technology to enhance teaching and learning. All members of the community appreciate that students, staff and parents have a shared responsibility to use the technology in a responsible manner in line with the ethos and values of the School.

Guidance for pupils is delivered via ICT lessons, Life Matters, and training on use of digital technology (school devices), and through general education: assemblies and tutor time. Sanctions for inappropriate use of IT are detailed in the relevant Rewards and Sanctions and Anti Bullying policies.

- The use of laptops and tablets during lessons requires permission from a member of staff. Devices should remain visible on desks. A reminder of the Traditions of St. Catherine's School in the Digital Classroom is posted in all Senior School classrooms and can be found here.
- For Sixth Form, phones should not be used while walking around school or at any time in the Dining Hall or lunch queue, except where instructed. Sixth Form may use phones in Sixth Form spaces only.
- Photos, videos and audio recording of any individual should not be taken without his/her permission. Care and discretion should be taken when selecting items to photograph and broadcast. No one should share an image of anyone else without their express permission.
- Great care should be taken about any photo showing a pupil in school uniform. Not only does the image reflect upon the school as well as the individual, but it may also raise safeguarding issues allowing strangers to identify where a pupil goes to school and thus to be able to contact them / meet them.
- All girls are expected to model good digital courtesy and treat each other respectfully with the proliferation of photographs and recordings. Specific permission should be sought before uploading recordings of any other person to the Internet or sharing via messaging platforms. Pupils must not make or proliferate manipulated images or videos which reflect or affect staff, peers or the School in unkind ways, or encourage others to do so. This is cyber bullying. Guidance is available from the Director of Digital Learning, Computing and ICT (Prep School), or from the Head of Sixth Form, Heads of Boarding Houses, the DSLs or the Deputy Head (Boarding, Culture and Community) as appropriate in the Senior School.
- Under no circumstances may photos or videos be taken in school changing rooms or toilets. Any such cases will be taken seriously and dealt with under the School's Behaviour Policies.
- The only permitted wireless network for use by students in school is "SC – Staff & Students". Checks are carried out at random and the use of other wireless networks at school constitutes a serious breach of this agreement.
- Students should not participate in chainmail or overpopulated message groups on mobile devices. All messaging in school must be identifiable and accountable.
- Students must not impersonate others or the School online, for example, by making fake accounts on social media or by contributing fake information to public websites. The School's wheel logo is subject to copyright and permission to use it on any digital communications must be granted by the Headmistress.
- Students must not share explicit, discriminatory, inflammatory or offensive materials.
- Students must not video or proliferate online chats/emojis containing content which may cause offence or harm (e.g. nude or semi-nude images, sexualized or aggressive messages/emojis etc.) either while in school, or outside school where identifiable as a St Catherine's pupil. This is a serious Safeguarding matter.
- Students must obey the age restrictions for all social media apps and websites while in school and whilst using school owned and managed devices whether that be in or outside School.

Part 3 – Filtering and Monitoring

Access to the Internet is filtered and monitored by the school firewall.

- 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.

Part 4 – Additional Guidance for Prep School

Early Years (Pre-School and PPI) - Use of Mobile Phones, Cameras and Electronic Devices

- Parents, guardians, carers and other visitors are not permitted to use their personal mobile phone, camera or any personal device, including smart watches, with imaging and sharing capabilities in or around the EYFS setting, without prior approval from the Head of Pre-Prep or Prep School Head.
- We use the secure online learning journal called Seesaw to share significant learning moments and achievements with parents. You will have an insight into your daughter's learning and can comment on any observation and upload your own photos and videos to share what your daughter is doing at home. To ensure the safeguarding of the girls, everything that is added to Seesaw can only be viewed by School staff and the parent of each girl.

PP2 to L3 (Years 1-6) – Responsible Access to Technology

ICT guidance for pupils is included in student planners and on display in each Form Room. This guidance is explained to pupils via the Form Teachers at the beginning of each term. The following additional rules are present for all students in the Prep School

- Privately-owned mobile devices are not permitted. Girls who travel to school by minibus, coach or public transport are permitted to bring a phone to school but must hand it to their Form Teacher at the beginning of the school day; it will be returned to them at the end of the school day.
- Students must ask a teacher's permission before using a computer or iPad.
- iPads are stored safely in the iPad charging stations in classrooms when not in use during the school day.
- Students may not use USB drives or print from computers or iPads without permission.
- Break times are 'screen free' time when iPads and computers are not to be used.
- Similarly, girls should not play games in lessons, breaks, or in the time between drop-off and registration or prep club/CAT Club.
- Students must turn on 'Do Not Disturb' on their iPads at the beginning of each day.
- Regular checks are carried out to ensure appropriate use and optimal functioning of issued devices.

A child-friendly amalgamation of all applicable rules is present in each classroom in the Prep School.

Part 5 – Additional Guidance for Senior School Boarders

The use of devices in boarding houses is subject to the following and at the discretion of the Head of Boarding and Heads of Boarding Houses:

- Boarders' mobile devices should be kept in the locker provided for each boarder, when not in use, and switched off. No device should be left charging on a bed, but on a hard surface in the dormitory and uncovered by paper/clothes etc.
- Boarders in U3-U5 must hand their mobile phones and other forms of digital technology into their Boarding Housemistress at night for safekeeping. This restriction is then at the discretion of the Boarding Housemistress for boarders in L5 and above.
- Boarders should only watch DVDs or download media of the appropriate legal age classification.
- If boarders are found using any digital technology after lights out, they will be confiscated by the Boarding Housemistress.

Part 6 - Cyberbullying

Inappropriate use of emails, social networking sites, texting or any form of digital technology could amount to child-on-child abuse and would be an infringement of the Traditions at St Catherine's. It will certainly be Cyberbullying if the content is offensive to or about another student. If this is reported to/discovered by a member of staff, the Schools' Anti-Bullying Policy will be invoked, and a full investigation undertaken. Pupils are advised never to post or text any material that they would be unwilling to share with a parent or teacher.

To prevent Cyberbullying, any unpleasant material or messages received should be preserved as evidence, reported immediately to a member of staff, and not responded to. Students should not feel worried about reporting incidents as this may help protect them and other students in the future. Parents should immediately screenshot and report to school anything their daughter may report to them as inappropriate behaviour online. It is everyone's responsibility to ensure that devices are used responsibly. Any improper behaviour is best dealt with as soon as possible.

The Whisper platform is available for anonymous reporting of concerns, difficulties or feedback on all aspects of school.

Part 7 – Device Checking

All student devices at school should be used responsibly and appropriately. To encourage this, while the school is in loco parentis during school hours, all devices (including smart phones, whether inside a Yondr pouch or not) are subject to spot checks or inspection while at school. The Education Act 2011 provides us with the authority to check the content of a personal device if there is a reasonable suspicion of harm or intended harm affiliated with the device.

The School may request the device be unlocked and may collect information about the use of the device, including apps, settings, screenshots and device activity. This will always happen with a member of the pastoral staff – wherever possible her tutor or housemistress - and the pupil present. Any suspicion of inappropriate use risks the removal of the device. Where necessary for further investigation or for parent awareness, the School may retain evidence from the device. If inappropriate use is discovered, parents will be informed. A device will only ever be looked at in the presence of the pupil.

Parents are encouraged to visit the community website for a complete collection of resources, advice and information regarding online safety.

Part 8 – Online Safety Guidance for Parents

The following points indicate how parents can make the Internet a safer place for children. The community part of the website has 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. The School cannot supervise the use of personal modern technologies outside School, and we depend upon parents' support in this area.

We strongly recommend that parents:

- monitor their own daughter's use of the internet and discuss with her its negative aspects. For younger girls, and until they have demonstrated that they can use devices properly, keep device use to family rooms, not bedrooms, so that you can see the sites she is using. Configure device restrictions to prevent private/incognito browsing, ensuring browsing history is available.
- pay attention to age restrictions and reputations of social media services and mobile apps such as Instagram, TikTok, WhatsApp and Snapchat. These are invariably restricted until at least age 13 and in many cases 16 or 18. Comprehensive guidance is available on the school community website. Parents should be aware that children often have a number of accounts on such sites, so that they have one which is suitable for parents to see, and one for friends etc.

- enforce the understanding that the parent, not the child, is the legal owner of the device and has the overarching right to control or remove it.
- encourage their daughter to share the Internet with them; ask her what sites she is visiting and why she likes them. Log on to the sites themselves so they can see what she is using and how the sites work.
- create a list of Internet and device house rules as a family. This can include sites and services that are off limits and how many hours can be spent using a device.
- remind their daughters never to give out any personal information to people they do not know. Encourage them to consider what information is inadvertently given out, such as time stamps and locations for regular events, such as weekend work, clubs etc., and in particular, discuss the Snap Map feature of Snap Chat with their daughter to check who can see her location whilst she is out and about.
- If the device has standalone Internet capability (e.g., 3G/4G/5G), the school cannot take any responsibility for Internet use; therefore, we ask parents to provide only non-enabled devices which can only access the Internet via the School's Wi-Fi, which includes a filtering and monitoring system. For mobile phones, parents may disable or minimize the data plan with the service provider.

We recommend that all personal devices and home Internet connections are configured appropriately for your daughter's age. For example, restrictions can be set to prevent adult apps being downloaded and block adult websites. Consult the community website and your Internet provider for guidance.

We politely request that parents respect data privacy when receiving communications or photographs of their daughter from School which may contain photographs/information regarding other students. Please do not proliferate or forward any such communications beyond the existing direct recipients.

Part 9 – Online Safety 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 or posting identifiable personal information on the Internet such as their real name, address, phone number, email address, school, and postcode. Remember that the visible contents of a photo may reveal this information.
- Ensure their mobile phone has the ICE (In Case of Emergency) numbers of their close family/next of kin programmed into it in line with emergency services' requests, to help them and hospital personnel in any emergency that renders them unable to give information in person.
- Be careful about putting photos of themselves or friends on websites. They should not send photos to someone they have met online or agree to meet them without the knowledge of their parents.
- Avoid chatrooms, video calls and emails with people they do not know. Learn how to block people and remember that many people on social networks are not who they say they are.
- If they receive any unpleasant material or messages, they should not respond. They should not be afraid to ask for help from a parent or member of staff if they see or hear about anything that worries them, or if they have done or said something they regret.

All pupils in U3 – L5 complete the Online Safety Alliance qualification each year. 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 should be used and kept secure by everyone.

We recommend that the free what3words app is installed on mobile phones in case of emergencies. This enables the emergency services to locate an individual within a radius of 3 x 3 metres.

Part 10 – Online Accounts

The creation and use of online learning platform accounts, as per the Guidelines for the Use of Digital Technology, incorporate the mobile workflow and communication solution which has been developed for the girls, along with ensuring that documents on their school devices are accessible and backed up safely.

We obtain specific parental permission for students to use online Microsoft 365, Google Workspace for Education and Seesaw accounts as part of this agreement, including common additional services from Google such as YouTube, Code First and Blogger which are not part of the education workspace agreement. You may review the privacy statements for educational institutions here:

https://privacy.microsoft.com/en-gb/privacystatement

https://workspace.google.com/terms/education_privacy.html

https://seesaw.com/privacy-security

These organisations respect the data privacy of schools in their educational software products, and all applicable agreements are scrutinised by the school to ensure fair treatment of personal information. Student data is not shared with third parties for commercial reasons or used for targeted advertising purposes.

Student information remains the property of the School. Where additional data processors are employed for learning platforms and other personalised online services, the school performs GDPR scrutiny and compliance checks before providing any student data. Information regarding organisations employed as data processors can be provided in accordance with the school's GDPR policy.

Please indicate your consent to the creation of these accounts and use of other data processors for educational services, by signature below.

Part 11 – Remote Learning

When attending lessons remotely, students should adhere to the following guidelines:

- Cameras should be on at all times.
- You should work in a space that is conducive to study and where you won't be interrupted, where possible.
- You should dress tidily and appropriately for work.
- You should conduct yourselves as you would in the classroom.
- You should not access other websites, social media or messaging while attending a lesson or film/record any part of the lesson. Address any questions about the lesson to the teacher through the chat or after the lesson by email. You may also request a Teams recording if necessary from the teacher.

Student and Parent ICT Agreement

Please complete and return a separate form for each pupil.

For Senior School, please return to Clare Woodgates, Senior School Registrar.

For Prep School pupils, please return to Kate Bishop, Prep School Registrar.

I confirm that we have read the ICT Policy, this Appendix, and other associated documents carefully. We have discussed this agreement in detail with our daughter and accept the terms of the Student and Parent ICT Agreement regarding the proper use of digital technology and agree to abide by them.

Pupil's Name: …… **Form**: ……

(Please print)

PARENT/GUARDIAN SIGNATURE: ……..

Date: ……..

PUPIL SIGNATURE (for pupils in Form I – Upper 6): ……..……

Date: ……..

Whole School ICT Policy - Guidelines for the Use of Digital Technology

APPENDIX 2 – ST CATHERINE'S SCHOOL STAFF E-MAIL CHARTER AND ICT AGREEMENT

Please read the ICT Policy and this agreement document in full then sign and date this form and return it to the Director of Digital Technologies.

This Agreement is an appendix to the Whole School ICT Policy - Guidelines for the Use of Digital Technology which will be reviewed annually and significant amendments/additions to either document will require this Agreement to be resigned. It is applicable to all St Catherine's staff including teaching and support staff, volunteers and casual staff.

Part 1 - Acceptable Use

All members of staff are provided with access to the School's telephone system, e-mail and internet to use primarily in connection with their work. Limited personal use of telephones, e-mail and internet is acceptable, but this must not interfere with the employee's work for the School or the work of other colleagues. Unreasonable personal use may amount to misuse of the facilities to which you have been given access and is a disciplinary offence. Serious misuse may amount to gross misconduct.

Staff must not give their personal e-mail addresses or personal telephone numbers to students unless this has been agreed with a senior manager and it would be in exceptional circumstances. Staff accompanying school trips should borrow the School Trips Mobile from the School Office or the Prep. School Office. In an emergency where a staff member does not have access to a school owned device, he/she should use their own device and hide their own mobile number by inputting 141 before dialling.

Staff Responsibilities

1. Staff must adhere to the stated policy as technology changes and must make best efforts to protect data and not indulge in activities that may compromise data, in line with enhanced awareness provided by the School regarding GDPR.
2. Staff save data to non-networked drives at their own risk. This includes local hard drives (normally called C:) as well as removable drives such as USB keys. If data saved on such drives is lost, the school makes no guarantee that such data can be retrieved.
3. Staff are prohibited from:
   - sending fraudulent, defamatory, abusive, obscene, sexist, racist, homophobic or otherwise unlawfully discriminatory or harassing messages.
   - accessing or distributing any material which is or may be thought to be pornographic, sexual in nature or otherwise offensive. The accessing or sending of any such messages or material may be considered a serious disciplinary offence and result in disciplinary action against the employee.
   - transmitting or downloading programs that have the intent of compromising information security or disrupting work.
4. Staff are required to notify the Director of Digital Technologies of any inappropriate content (such as material of a pornographic, fraudulent, defamatory, abusive, obscene, sexist, racist, homophobic or otherwise unlawfully discriminatory or harassing nature) suspected to be stored inside the School's digital bounds.
5. Staff are required to use official School e-mail systems when communicating professionally with colleagues, parents or pupils and should *never* using a home/private e-mail address.
6. As part of the School's ongoing commitment to effective use of ICT, and in recognition of our status as an Eco School, we require all staff, including those on permanent or temporary contracts, to keep abreast of information sent via the School's e-mail system. This is expected as part of your job responsibilities. Details on how to access your School e-mail are available from the IT Support

Department. Training on the most effective use of Outlook is offered by a member of the IT Strategy Group if requested.

Enforcement

1. The school will audit resources periodically to ensure that software and computer configurations comply with policy.
2. If any part of this policy is violated, the employee's access rights to the computer systems may be restricted or removed as decided by the Headmistresses.
3. Staff must attend ICT training where directed. For academic teaching staff, keeping up with developments in teaching and learning using technology is an important and expected part of professional CPD.
4. The school may employ practice emergency drills or simulated cyber-attacks as part of maintaining and improving ICT awareness. All staff share responsibility for safeguarding the integrity of the ICT systems through remaining alert to such potential threats and taking notice of updates provided by the Director of Digital Technologies at staff meetings or in the routine e-updates.

Early Years (Pre-School and PPI) - Use of Mobile Phones, Cameras and electronic devices

1. Staff may only use their mobile phones in the Pre-Prep office, staffroom or an outside area out of the sight of pupils.
2. Staff working within the EYFS classrooms must store their mobile phones in the Pre-Prep office or staffroom.
3. Photographs taken for the purpose of recording an EYFS pupil or group of pupils participating in activities or celebrating their achievements must be taken on a school device and stored appropriately within the school system.

Part 2 – Monitoring

The School will not undertake any form of unnecessary e-mail, Internet or other communication monitoring but reserves the right and has the capability to do so if necessary and authorised by Senior Management. Where monitoring is necessary, this will be carried out in accordance with the relevant statutory provisions and to the extent permitted. Such monitoring is for Safeguarding or business reasons, to enable the School to carry out its role as an employer and to comply with its duty of care towards pupils and employees. In particular, the School monitors e-mail, Internet access and the network in order to:

- ensure the proper safeguarding of its pupils
- prevent or detect crime e.g. cyber-attack, ransomware etc.
- investigate or detect unauthorised use of the e-mail or Internet or use in any way contrary to this policy or to ensure the effective operation of the network (for example to detect viruses)
- carry out monitoring by way of spot checks rather than engaging in any form of continuous monitoring unless by way of an investigation into suspected misuse of the e-mail/Internet.
- monitor, by automated means, to reduce the extent of information available to any person other than the parties to a communication.
- target any monitoring to areas of known risk, rather than any form of widespread monitoring.
- prevent misuse which poses a significant threat to the students, school property or administrative efficiency.

The School reserves the right to carry out monitoring for any other reasonably justified purpose.

Any use of zoom, including for the teaching of lessons or for meetings, will be recorded and stored but will not normally be viewed except in cases of allegations made against members of staff.

Checking Business Communications

It may be necessary to check Staff e-mail accounts for business communications during Staff absence. The School will avoid, where possible, opening those e-mails that have a heading and/or address which suggest they are private or personal communications. Staff should therefore use a system to indicate private or personal communications and encourage those sending such e-mails to do the same.

When Staff know they are to be absent from work they should activate an out of office outgoing message indicating the length of absence and who may be contacted in their absence. Suggested 'house style' proformas exist in the Staff E-mail Charter for the wording of such messages. Please note that 'out of office' may be set with a message for external readers and a different one for internal readers.

Part 3 – Social Media

The recommended guidelines for the use of social media for the whole school are located in the document - 'Guidelines for the Use of Digital Technology'.

St Catherine's School employees must not "befriend" current students on social media sites such as Facebook. Careful consideration should also be given to "befriending" former students as they may still have other friends or sisters within the school and comments expressed under the impression of a 'private conversation' may still end up being shared into a more public domain. The same consideration applies to the use of instant messaging and personal email addresses. Staff who regularly require contact with alumnae of less than 5 years should alert a DSL and state the purpose. Staff requiring contact with a pupil by any other means than school email should alert a DSL.

Part 4 – Information Security

Purpose

The purpose of establishing this information security policy for St Catherine's School is to protect school information and IT related assets while allowing: 1) information transfer, 2) e-mail communication, and 3) controlled access to the Internet and web-based information. It also defines policies for protecting data within the School and addresses the confidentiality, data integrity, availability, accountability and responsibility issues that each staff member must be aware of and comply with while working for St Catherine's School.

Threats to be aware of

1. Malware introduced to the network by e-mail, web browsing, downloads, portable drives and other media.
2. Loss of private/personal information through phishing and other internet-based scams.
3. Unauthorized login into computers by learned or hacked usernames and passwords.
4. Unauthorized network access to server and workstation computers.
5. Unauthorized physical access to school servers that may result in inadvertent or malicious shutdown, damage or login access to the server.
6. Unauthorized access to data by a user because of lack of file protection.
7. Loss of data integrity of confidential data during network transfer (i.e. data tampered with during transmission).
8. Theft of disks, tapes and USB keys containing confidential data
9. Unauthorized tampering with network resources that can lead to the loss of network availability.
10. Loss of power to critical IT components.

11. Theft of data through personal mobile devices which have online or offline access to School resources.

Confidentiality

1. It is not recommended that confidential data is ever taken off site. However, should this be absolutely necessary, and approved by the IT Support Department in each case, data should be securely protected by adequate measures such as strong passwords or encryption. Encrypted USB keys are available from the IT Support Department as well as guidance on how to encrypt your own USB device.
2. Most data is accessed centrally via network credentials and the relevant account should be logged off or protected by an equivalent password, on the personal device.
3. It is the staff member's responsibility to ensure adequate privacy barriers exist between apps and documents and passwords, where a personal device is communal and shared between family and friends.

If users have any concerns or issues to report, they should immediately contact the Director of Digital Technologies regarding information security, or the Designated Safeguarding Lead (DSL) or DDSLs regarding student safety. The DSL is the Deputy Head, Staff (Prep School); DDSLs are Senior School Housemistress (Senior School), Head of Pre-Prep (Prep School) and Head of 6th Form Boarding (Senior School)

Integrity

1. Only administrator accounts belonging to the IT Support department have access to all network areas.
2. All file transfers of confidential data must check for the integrity of the data.
3. All personal desktop/laptop IT systems must have anti-virus software present that supports real-time scanning on all disks and portable drives.
4. Confidential or dense collections of personal data must be encrypted during transfer. Support from IT should be sought, for example to send encrypted e-mails to external data processors.

Part 5 – Staff Email Charter

Email is an essential modern communication tool. It makes the School more efficient, allows colleagues to be more informed, and enables us to support parents much more effectively in the education of their girls. However, it can be unwieldy. Keeping to the protocols below will assist in keeping email effective and reduce administrative burden.

Core Principles

1. Anything you commit to email you should be happy to be made public or to place on a girls' file Named individuals in e-mails and those identified by their initials are entitled to a copy of the e-mail.

2. Use a meaningful and directional subject line and appropriate recipients

Use the subject line to help the recipient get your point quickly and assist in email searching and filing. Completing discussions by email is a good way to tie things up so that they are obvious when you look back on them years later. When a discussion changes topic, change the subject line and amend the recipients to those who need to pursue the topic. cc'd recipients are not expected to reply unless they have some significant new information or idea to add.

3. Think of the recipient's time when composing

Make the email short and easy for the reader to process; strike a balance between brevity and courtesy. If you are playing email ping-pong about a topic, or struggling to get the tone right, pick up the phone. The tone of e-mails is easily misread and talking served the world well for quite a long time. After the discussion, key points can always be summarised.

4. Develop habits that will minimise errors, mistakes and delays

Re-read carefully and beware of auto-correction errors. Habitually check the recipient list on the way to the send button. Consult a senior colleague in isolation if you are not sure how to proceed. Avoid open ended questions e.g. "Thoughts?" in favour of a choice e.g. Shall we talk about this? or Shall I deal with it myself?

5. Remain vigilant for anomalies and cyber threats

Email is a major cyber-threat and fraud-risk. Check hyperlinks in e-mails before following them by hovering, to check the website is legitimate. Perform the same check for reply addresses and think twice if there is anything being requested that could potentially be anonymous and fraudulent. Malicious e-mails are invariably self-evident.

Professional Standards & Expectations

- An appropriate signature should be coordinated with your Head of Department and with any automatic school footer. There is no need for a salutation on internal emails. All information re. sender and recipient is provided electronically.
- When emailing external recipients on behalf of the School, use the correct formal salutation – Dear Mr/Mrs/Dr/Ms *** - and sign off: yours faithfully/yours sincerely as appropriate to the situation. Do not use first names in correspondence with parents, regardless of how well you feel you know them.
- During school holidays and periods of absence, your Out of Office messages (you have the option to write an external and an internal message) should make your likely responsiveness clear to the sender, and redirect enquiries to a colleague, department or school office, such as:
- *I will be away from School until <date> and will have no access to email during this time. If your enquiry is urgent, please contact the School Office on schooloffice@stcatherines.info where someone will be able to assist you.*
- Retain e-mails for future enquiries. You may sort e-mails into subfolders or ensure they are retrievable by meaningful search terms and it is not necessary to keep an empty inbox. Beware of counter-intuitive workflows such as marking old e-mails as unread, which could be misleading upon inspection.
- It is reasonable to be expected to respond to an easy email from parents within 24 hours. If you need more time, send a holding email acknowledging the enquiry. If something is truly very urgent, call or find the person instead of using email. See also the protocol for handling unpleasant/rude/offensive emails from parents published by the Headmistress in Sept 2019.
- It is reasonable to expect a response time within 48 hours from colleagues, after which remind the recipient politely on the assumption that it will be because of a full inbox/teaching day/diary. For SLT, talk to the PA after no response to the first reminder, not the colleague.
- When emailing at the weekend, all agree that this is not pressure but someone dealing with their workload and therefore the writer does not necessarily expect a response over a weekend. Responses within the boarding staff team on duty might be an exception. Where quantity or hours are anti-social, make use of email delayed delivery features where possible. It is acknowledged

this is less easy on an iPad. Remember that to ensure delayed emails are sent at the right time from a PC, the PC must be on and Outlook open.

- Ensure that any attached outgoing documents are saved with School house-style heading and footer (which includes title, date, originator etc.) before attaching. Anything with legal implications should be sent via a signed letter. This includes absence notes from parents explaining days off school. Emails printed off and signed suffice, too.
- Remember to CC any relevant email threads to pupil.filing@stcatherines.info or preppupil.filing@stcatherines.info e.g. with parents etc. or send to the relevant School Office email address.

Footnote: *The St Catherine's Email Charter is based on a document originally created from a blog post by TED Curator, Chris Anderson, and TED Scribe, Jane Wulf. They describe it as a private, non-commercial initiative. A simple 'idea worth spreading'. More than 45,000 people read the post and it generated hundreds of tweets.*

Part 6 – Devices

Teaching staff operating in classrooms are equipped with a premium mobile device for optimal delivery of digital materials. Staff are trained and equipped in support of ongoing technology initiatives and acknowledge personal responsibility for the care and dedicated professional use of allocated devices.

Staff Acknowledgement of St Catherine's School ICT Policy

This form is used to acknowledge:

- Receipt of and compliance with St Catherine's School ICT Policy – Guidelines for the use of Digital Technology.
- St Catherine's School Staff ICT agreement.

I confirm that I have read and agree to abide by the terms laid out in the St Catherine's Whole School ICT Policy document and relevant appendices.

Employee Signature	
Department	
(paper signatures only) Print Name	
(paper signatures only) Date	