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

Appendix 2 – St Catherine's School Staff E-mail Charter & 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 re-signed.

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 his/her 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, they 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 pupil ***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 ICT Development Committee 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.

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 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:

- 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.

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.

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 should 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 e-mail 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 Senior School Housemistress (Senior School) or Deputy Head, Staff (Prep School) regarding student safety

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 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 *** - and sign off: yours faithfully/yours sincerely as appropriate to the situation.
- During school holidays and periods of absence, your Out of Office 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.
- 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 SMT, talk to the PA, 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 e-mail delayed delivery features.
- Ensure that any attached outgoing document 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. Combined SMT worked from this basis to create this document during Autumn 2012 for launch in January 2013. The Email charter was revised and updated in January 2018 by the Director of Digital Technologies and incorporates guidance relevant to GDPR..

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 agreed to abide by the terms laid out in the St Catherine's Whole School ICT Policy document and relevant appendices.

Employee Signature	
Employee Name (please print)	
Department	
Date	