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

Appendix 2 – St Catherine's School Staff 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

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 it has been agreed with a senior manager. Staff accompanying school trips, who have obtained permission of SMT, may use their mobile number as a point of contact for pupils and parents. If they do not wish to use their own phone they should borrow the School Trips Mobile from the Facilities Office or the Prep. School.

Configuration Issues

1. A suitably configured firewall separates school workstations and servers from the Internet.
2. Access to internal servers from the internet is restricted by the firewall.
3. Publicly accessible servers such as a web server and e-mail server are securely configured.
4. All School computers will have up-to-date anti-virus software installed.
5. Data communication between domain controllers may be encrypted.
6. All software and hardware installations must have their default passwords changed regularly, where applicable.

Violations

If this policy is violated, then the employee's access rights to the computer systems may be restricted or removed as decided by the Headmistresses.

Part 2 – Monitoring

The School shall 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 shall 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
- 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.

Part 3 – Information Security

Purpose

The purpose of establishing this information security policy for St Catherine' 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.

Confidentiality

1. School servers are located in a secure physical location with access only by authorized staff.
2. All users must have a separate user account and password that must be kept confidential, save on the termination of employment the account will be closed down.
3. The password policy requires passwords to be a minimum of 8 alphanumeric characters long and automatically requires the user to re-set their password every 90 days. Please see the 'Guidelines for Digital Technology' document on the correct procedure on how to select a secure password.
4. Users may not share accounts except where expressly permitted by the IT Support Department
5. All user accounts will use password-protected screensavers except where expressly permitted by the IT department.
6. Users must not access another user's data without permission. Each server must have a file protection system that restricts user access to his or her own files. Exceptions include a user belonging to a group that has file access via group file permissions.
7. It is not recommended that confidential data is ever taken off site. e.g. pupil details. However, should this be absolutely necessary, and approved by the IT Support Department in each case, data must be encrypted. Encrypted USB keys are available from the IT Support Department as well as guidance on how to encrypt your own USB device.

If users have any concerns or issues to report, they should immediately contact
Director of Digital Technologies regarding information security
Senior School Housemistress (Senior School) or Deputy Head, Staff (Prep School) regarding student safety

Integrity

1. The administrator and alternate administrator accounts are the only accounts with access to all files.
2. All file transfers of confidential data between machines must check for the integrity of the data.

3. All systems must have anti-virus software present that supports real-time scanning on all disks and portable drives.
4. Confidential data may be encrypted during transfer.

Accountability

1. All account security events are logged.
2. All new software deployed must be authorized by IT staff.
3. All connections through the firewall are logged.

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.
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. Copyrighted software must be used in accordance with the software licence.
4. The hardware configuration of a desktop workstation must not be changed without approval from the IT department.
5. 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.
6. Staff are required to notify the Director of Digital Technologies or Network Manager 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 on the Network.
7. Staff are required to use official School e-mail systems only when communicating professionally with colleagues, parents or pupil *never* using a home/private e-mail address.
8. 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 and VPN from home are available in the ICT folder on the Y drive and from the Network Manager.

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 has been violated then the employee's access rights to the computer systems may be restricted or removed as decided by the headmistress.

Part 4 – 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 sites such as Facebook. Careful consideration should also be given to "befriending" ex-students as they may still have other friends within the school and comments expressed under the impression of a 'private conversation' may still end up being shared into a more public domain.

Part 5 - Remote Access

St Catherine's School employees have the facility to access the School network resources whilst away from school via our remote desktop facility. Staff are required to be vigilant when accessing systems remotely. Computers or other digital devices should not be left unattended when connected.

1. Remote users will be logged out of the remote desktop if left unattended for fifteen minutes.
2. Pass additional security checks i.e. door code

3. Staff must make sure they are not being overlooked by anyone, even family, when accessing confidential data.
4. Network passwords should not be disclosed to family members nor should they use the School system.

The school provides broadband wifi internet to all resident accommodations on the school site and are asked to sign an agreement regarding use of school IT services.

Staff are advised not to share other school services which access the school's data with their spouses. They must not share their school username and password.

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	