St Cecilia's

R. C. High School

POLICY FOR DIGITAL COMMUNICATIONS

Approved: October 2018

Next Review Date: October 2019

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which have changed the way we all work. The digital world has improved communication and the way we can share work, ideas and collaborate on the same projects. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This policy is set out to establish best practice within school and ensure fair use of technology by all members within St Cecilia's RC High School.

All parties within St Cecilia's RC High School should follow this policy when using the ICT systems provided within school and outside of school to keep a high level of professionalism.

Contents

1.Email and digital Messaging Policy

The proliferation of email traffic over the last few years has allowed us to communicate more efficiently and effectively. We are entering an even greater period of email use as students and parents now also have the ability to benefit from this form of communication. In order to ensure that all parties (staff, students and parents) continue to find email use effective and not too burdensome, we ask that the guidelines listed below are adhered to.

<u>Email etiquette</u>

- Try to decide if you are sending an email for the purposes of information giving, or for some other reason. Information giving is definitely the best use of email - but be careful with any other purpose, particularly any that involves emotion!

- Avoid using email for complaining or venting – this is not an appropriate use of the medium. Don’t use email as an excuse to avoid personal contact. A simple ‘rule of thumb’ is to ask yourself if you would say what you have written directly to the person.

- Humour can also be easily misinterpreted, especially sarcasm. Try to avoid it unless you know the recipient very well.

- Try to keep the email as a whole brief, and to include a clear subject line as a header so people can identify swiftly whether or not it is relevant to them.

- Double check everything you write, as errors can be harder to spot at certain times of the day, when you are rushing or when you are occupied by other things.

- Check to whom you are sending the email before sending it. Bear in mind that the ‘Reply to all’ option should only be selected if you really need everyone on the distribution list to see your reply. This should be used sparingly.

- Please also think carefully before using the CC option. Only use it when necessary and in the understanding that it does not require a direct response but is for background information only.

- Make sure that you are clear as to what the purpose of the email is. Do you require specific action, or is the email for information only?

- Please note that defamatory or abusive emails should not be responded to. The receipt of such emails should be reported to your line manager.

- If you send an email out of hours please don’t expect a reply until the next working day as staff are not expected to read emails during these times.

Email on Mobile Devices

Work email should only be accessible on a secure, password protected, encrypted device.

Staff should only access emails via **Microsoft Outlook** app available on both android and the apple store.

Staff are not permitted to have access to emails on their mobile devices if a device password or fingerprint protection is not set.

Should staff lose their mobile device containing school emails, whether personal or school owned device, staff must report this to the Data Protection officer and Network Manager within 24 hours.

St Cecilia's RC High School reserve the right to remotely wipe ANY mobile device containing Work emails, for the purpose of preventing a data breach, for example a lost or stolen phone.

2. Digital Storage and Data Retention Policy

2a. Data Storage

Information Technology and computers have become vital within the education sector over the past few years, and as the demand for technology increases, so does the need for larger data storage solutions.

Although we have adequate resources in place, staff should be mindful of how much storage they are consuming on the network as it is a finite resource shared across the school.

Staff should follow these rules along with the ***ICT Acceptable Use Policy***

- Personal files with no relation to work such as photos, videos, movies, MP3's and other files are not permitted on the network. These can be stored on OneDrive for backup if required.
- Illegal or copyrighted materials must not be stored on the network.
- Staff should delete old files no longer required, especially Photos and Videos of past students.
- Staff shared drives is for sharing of resources only, anyone can view these files and could potentially delete them. Staff should use their home areas for storing of work materials you don't wish to be shared.
- Confidential data should not be shared on Departmental folders, unless absolutely necessary and stored in a specific protected folder created by the IT Department.

- At the end of each term, staff should delete any unwanted files they know they will not need again especially old work from past students who have now left.
- All USB pen drives containing data must be encrypted by the Network and Data Manager.

2b. Digital Account/Data Retention and Deletion

The following will set out how long we keep files and folders on the network before being deleted, for both staff and students.

Students

Retention Period: **12 Months**

- Student accounts are disabled on the day of the final Year 11 exam and archived for roughly 12 months.
- All files and folders relating to student accounts, including coursework, will be kept for up-to 12 months to allow time for ex-students to request their personal work or to allow a re-mark of coursework should evidence be needed.

Staff & Temporary staff

Retention Period: **3 months**

- Staff accounts are suspended at 3:05pm on their final day of contracted work. After this time, access to emails, home area and shared resources will be restricted.
- Files and folders in staff home areas will be deleted 3 months after termination of employment date.
- OneDrive files will also be kept for 30 days, after this they will be deleted.
- Staff should delete all files belonging to themselves before termination of employment.
- Staff are permitted to keep files on Staff shared folders after they leave, providing the files will assist Teaching & Learning and be used by current staff.

Emails Retention & Deletion

Emails will be deleted automatically after 18 months from your mail box for both staff and students. This is to reduce the risk of a potential databreach and should be done anyway as 'good housekeeping'. Any emails you want to save need to be saved in a new folder.

3.Remote Access Policy

For staff with Internet access at home, it is possible for them to gain remote access to their school computer. Access is also available to the departmental folders and staff can also access Sims.net for submitting reports etc

Access is not a right and may be withdrawn at any time, without prior notice and without reason. Any violation of the terms, as set out may result in the removal of your access outside of school.

Terms of the Agreement

When using any remote access tools staff are bound by the Staff Acceptable Use Policy alongside the rules below;

The uploading of any files not directly related to your schoolwork is strictly forbidden, as are files of the following nature:

- Any virus infected files;
- Executable files (e.g. computer software, self-extracting archives);
- Command execution files (e.g. JAVA scripts, batch files);
- Files containing any defamatory or unlawful text and/or images;
- Personal music files should not be stored on the system due to copyright issues.

No attempt will be made to interfere with the correct operation of the system and no attempt will be made to access anyone else's school account or attempt to deny anyone else access to their account (denial of service) by any means.

Antivirus

Any computer/terminal you wish to use whilst accessing the school's computer system must have an approved Anti-Virus package installed. If you do not currently have any Anti-Virus software installed, one must be installed before you will be granted remote access. Once installed, the software must be running at all times you are connected/communicating with the school's computer system.

You will undertake all reasonable measures to ensure your anti-virus software is kept up-to-date with the latest software updates and virus detection databases. The following packages are approved:

- Avira Free Antivirus (Free)
- Symantec's Norton Anti-Virus
- Kaspersky
- Panda Free Antivirus
- Windows Defender (Windows 10) (Free)
- Microsoft Security Essentials (Free)

Sims access must be used by yourself and yourself only. Confidential data can be accessed from within Sims and this must be kept private at all times. You must not give your password out to anybody else. It is important to respect and adhere to Data Protection Laws when accessing sensitive date at home.

Under NO circumstances must you leave your computer/terminal unattended whilst accessing ICT services from outside of school.

By using Remote Access you are aware that you are fully responsible for ALL actions carried out in and/or with your account.

Data Protection

The remote access system allows staff to remote directly into the school network with access to files, folders, office suite and SIMS to avoid the need to download any files to the local laptop or pc.

4. Mobile Phone and Personal Devices Policy

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office and/or via landlines located in each Faculty or by walkie-talkies where provided. If you are in a location where communication is not possible (e.g. fields, woods) and you do not have a walkie-talkie then staff should carry mobile phones for emergency use only.
- Staff should have their phones on silent or switched off and out of sight (eg in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (eg classroom, corridor, playground).

- Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g in office areas, staff room, empty classrooms.

- Staff must security protect access to their phone.

- Should there be exceptional circumstances (e.g acutely sick relative), then staff should make the Headteacher and office staff aware of this so messages can be relayed promptly.

- Staff should report any usage of mobile devices that causes them concern to the Safeguarding team or HOY.

Mobile Phones\Personal Devices for work related purposes

We recognise that mobile phones provide a useful means of communication on off-site activities. However, staff should ensure that:-

- Mobile use on these occasions is appropriate and professional

- Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the School Mobiles Provided.

- Where possible, staff should not use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras, ipads or school phones. Where this is not possible, photos/videos should be transferred to the school network ASAP and the images deleted off your phone immediately.

- School Data should not be stored on your personal devices and as stated in the email access on phone section access to the One Drive app must be on a password, encrypted device and also fingerprint protection where possible.

- If a personal device is lost that contains data, it must be reported to the DPO. St Cecilia's have the right to wipe personal devices in such circumstances.