



St Cecilia's
R. C. High School

Discover • Develop • Rejoice

Digital Communications Policy

**Reviewed: September 2023
Next Review Date: September 2024**

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
2. Digital Storage & Data Retention Policy




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.

Email and messaging etiquette includes all school messaging applications including Edulink

Staff Email

-  Try to decide if you are sending an email/message 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/message 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.
-  Staff are not expected to reply to messages from parents on Edulink out of working hours.

To pupils

Staff should ensure that they use pupils' school email addresses ONLY. The use of personal addresses would leave staff members extremely vulnerable. Therefore, for the protection of members of staff, pupils' personal email addresses MUST NOT be used.

Parent to staff email/Edulink

When a concern or query arises, parents should communicate with the form tutor or head of year in the first instance either by telephone through the school office or emailing info@st-cecilias.lancs.sch.uk.

Parents are requested not to email/message members of staff directly even if their email addresses are known, unless there is a pre-agreed arrangement between the teacher and the parent. We request that parents refer all school-related matters back to the school, and do not approach other pupils or contact other parents directly about such issues. We are interested in working with parents to create solutions. Contacting other pupils or parents can complicate and even exacerbate problems, whereas referring a concern immediately to school will expedite a resolution.

Spam/Phishing Emails

Any emails received asking you to 'Check your account' or 'Provide bank details' are more than likely malicious emails designed to gain access to your accounts or bank accounts, emails like this should be deleted immediately. **Do Not Click Any Hyperlinks.** If anybody is unsure please forward to the Network Manager and they will advise accordingly.

Periodic 'Phishing' tests will be sent out by the Network Manager.

Email/Edulink 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/Edulink on their mobile devices if a device password or fingerprint protection is not set.

Should staff lose their mobile device containing school emails, Edulink 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. By using work emails on your phone, you agree to these conditions.






2. Digital Storage and Data Retention Policy

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.

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: **6 Months (reduced from 12)**

- 🏠 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: **30 Days (reduced from 3 months)**

- 🏠 Staff accounts are suspended at 3:15pm 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/ SharePoint 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 mailbox for both staff and students. This is to reduce the risk of a potential data breach and should be done anyway as 'good housekeeping'. Any emails you want to save need to be saved in a new folder.

Policy Decisions

Authorising Internet access

- All staff must read the full '**Digital Communications Policy**' including the '**Staff Acceptable Use Agreement**' before using any school ICT resource.
- ICT access, including internet access is given at the school's discretion and can be revoked at any time.
- Pupils will be asked to sign and return a consent form when their child enrolls at school.