

ICT Acceptable Use Policy September 2025

This policy applies to all staff, students and visitors of Cardinal Allen Catholic High School, Fleetwood and those that use the school's online services remotely.

Policy Statement

Cardinal Allen Catholic High School IT facilities must be used correctly and not misused or abused by users. This includes electronic services such as Email and the Internet. All staff and students should be committed to conforming to good practice in this area. Use of the school's IT facilities implies acceptance of the conditions of use. This document sets out current policy and practice; this document is reviewed regularly and can change without notification.

Scope

The following regulations apply to users of all IT facilities and online services including learning resources owned, leased or hired by the school, all users of such facilities and resources on the school's premises and all users of such facilities and resources connected to the school's networks.

Staff and students should note the consequences of failing to comply with these regulations; particularly that disciplinary action may be taken by the school for failure by a user to comply with them.

Definitions

Portable Computers - Laptop and Notebook computers owned, leased or hired by the school.

Desktop Computers - Static Desktop and Workstation computers owned, leased or hired by the school.

Users - All staff and students of the school and others outside who have been given permission to use the school's IT facilities and learning resources.

Facilities - IT facilities located in the school and services which are available online (including the Virtual Learning Environment, Email and any additional services which may be added), including networks, servers, desktop computers and portable computers, together with the software and data stored on them. Any IT use carried out on equipment connected to the school network, whether or not this involves the use of a school-based, personal or school owned computer.

Learning Resources - All learning resources including (but not exclusively) text, video, audio which are available to the school's users either on the network or the Internet.

Relevant Legislation

Users must comply with all UK legislation relating to the use of information, computers and networks. These laws include, but are not limited to:

- a. ***Data Protection Act 2018. This act makes provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.***
- b. ***Copyright, Designs & Patents Act 1988. Copyright material includes literary works (including computer software), artistic works (including photographs), sound recordings (including music), films (including video) and databases.***
- c. ***Computer Misuse Act 2022. The act provides safeguards for computer material against unauthorised access or modification.***
- d. ***Privacy and Electronic Communications (EC Directive) Regulations 2003. These regulations prohibit the sending of unsolicited marketing, offensive or threatening Emails, SMS or text messages. In addition, the regulations control the use of 'cookies'.***
- e. ***Fraud Act 2006. The Act prohibits 'phishing' whereby official-looking Emails guide unsuspecting users to fake websites (e.g. fake bank websites) in order to steal their login details. Creating or possessing software to enable this activity is also an offence.***

Use of Facilities and Learning Resources

Personal Use

The school's IT facilities are provided for educational, administrative, research and personal development use by staff in the course of their employment and by students in the course of their education.

Students are not permitted to use the school's IT facilities for personal use. Limited personal use of certain facilities is permitted during personal time for staff. Any such use must not interfere with the employee's own work. The school reserves the right to withdraw this benefit either individually or collectively at any time. In such circumstance the school will endeavour to give reasonable notice of its intention to withdraw such benefit.

Where the school becomes aware of a specific type of personal use which affects the efficient operation of its IT facilities, the school will take appropriate steps to withdraw, without notice, access to the relevant facility or resource. Non-exhaustive examples of this include barring access to certain technology or Internet resources such as web sites, news groups or other Internet resources. Users who have a legitimate requirement to access such withdrawn resources should discuss the matter with the Headteacher.

Commercial Use

Use of any of the school's IT facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a student's course of study at the school or a member of staff's legitimate activities) is prohibited, unless the user has explicit prior written permission of the Headteacher and an appropriate charge for such use has been contractually agreed between the other party and the school.

Movement

School IT facilities, with the exception of portable computers should not be moved or disconnected without the prior agreement of the IT Manager.

Connection - Network Access

Students must not connect any personal device into the school's network or other IT facility.

Staff must ensure that any personal devices that connect to the school's network are both virus free and secure.

Damage

Users must not cause any form of damage to the school's IT facilities, software, or to any of the rooms and their facilities and services which contain that equipment or software. The term 'damage' includes any unauthorised installation of hardware or software.

Security

All of the school's IT facilities have anti-virus protection installed. Users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the school to prevent this. Users must not attempt to penetrate the security and/or privacy of other users' files.

Spam and Mass-circulation

Spam is usually defined as unsolicited electronic messages (using Email, SMS, Instant Messaging or other means) sent in bulk. Users must not use school IT facilities to send Spam.

Illegal and/or Offensive Material

Users must not use school IT facilities to access, produce, obtain, download, store, view, share, or distribute material (including images, video, text or sound files) which is either illegal under UK law, in breach of copyright law and/ or can reasonably be judged to be offensive, obscene, indecent, abusive or likely to incite racial hatred. The only exceptions would be where such material, which may be judged offensive, is essential for research or teaching, is permitted by law, and prior permission has been granted by the Headteacher.

Discrimination

Users must not use the school's IT facilities to place, disseminate or receive materials which discriminate or encourage discrimination on, for example, the grounds of gender, sexual orientation, disability, age, religious belief, race or ethnic origin.

Defamation

Users must not use the school's IT facilities to publish any information which they know or believe to be untrue including any information which may cause offence.

Passwords & Security

Protecting the school's computers, systems, data and communications from unauthorized access is of paramount importance; strong passwords play a critical role in this process especially when systems can be accessed remotely. All use of the school's user accounts, desktop computers, notebook PCs, servers, online services and electronic communications must conform to the following rules both locally and remotely.

No passwords are to be spoken, written, e-mailed, hinted at, shared or otherwise made known to anyone other than the user involved.

No passwords are to be shared in order to “cover” for another individual who is out of the school or otherwise indisposed. Instead, contact ICT Services for a temporary account.

No accounts must be shared.

Passwords should never be physically written on paper nor written and concealed near a workstation or stored electronically.

All passwords must be changed when requested and must never be reused.

Password Complexity

Passwords for all end user systems must meet the following criteria:

Passwords must include:

At least eight characters in length.

Lower case letter (a-z)

Upper case letter (A-Z) Numbers (0-9)

Symbols: i.e. !, @, #, \$, %, ^, &, *,) and (whenever possible.

Passwords must not include:

Any portion of your name

Any portion of your address

Date of birth

All staff computer screens must be locked to prevent unauthorised access when unattended.

Monitoring of IT Facilities

In order to protect the security and working of the school's IT facilities & users, daily monitoring of IT facilities will take place. This is particularly likely where there are indications of abuse of systems, or that individuals may be using systems in excess of their authority. Files, messages, Emails and user account information may be intercepted, monitored, recorded, copied, audited and inspected.

Confidentiality

Absolute confidentiality cannot be guaranteed. Any Emails or files, stored and/or sent or received may be accessed by individuals other than the one to whom it was intended for, whether by accident (e.g. a

computer that has not been locked) or design (e.g. an Email may need to be opened to diagnose connectivity problems which have been brought to the attention of ICT Services.). Emails and files cannot therefore be regarded as totally private or confidential. Personal Email messages and files should be written remembering this possibility for third parties to review the content. In the case of external (Internet) Email, there cannot be an absolute guarantee of security. Such Emails can potentially be intercepted and read by third parties without schools knowledge. Messages of particular confidentiality or sensitivity should be sent by an alternative medium.

ICT Services have total administrative access to all of the school's IT facilities. They have the right to monitor and access all IT resource; this includes any saved files. Any misuse of IT facilities found will be reported to the Headteacher.

Internet Access

Internet access is provided for educational, administrative, and research purposes. It should be noted that users of the Internet do not have a right to confidentiality or privacy when using or accessing the school's IT facilities. The Designated Authority monitors and reviews network logs maintained in order to ensure compliance with school policies and UK law. The school uses monitoring software to track usage. This software records details of every web site visited, along with the relevant user name and date/time, and produces regular reports for monitoring purposes. Misuse, or visits to sites of an improper nature will automatically be reported to the Headteacher.

Email

The school reserves the right to retrieve the contents of messages for the following purposes:

to monitor whether the use of the e-mail system is legitimate and in accordance with this policy; to find lost messages or to retrieve messages lost due to computer failure; to assist in the investigation of wrongful acts; to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. The school will not routinely monitor e-mail messages. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the school has reason to believe that the systems may be being used in breach of this policy.

School email will require 2FA via a mobile device to login outside of school. The end user must be responsible for this authentication.

Files

The school reserves the right to retrieve the contents of files for the following purposes:

to monitor whether the use of the storage medium is legitimate and in accordance with this policy; to find deleted files or to retrieve files lost due to IT facility failure; to assist in the investigation of wrongful acts; to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. The school will not routinely monitor files. Spot checks or tailored searches may be undertaken in the context of disciplinary proceedings (whether actual or contemplated) or where the school has reason to believe that the systems may be being used in breach of this policy.

Storage – Personal Folder and Departmental Shares

Each user receives a personal folder, which is private to them and accessible via the network. A maximum quota is imposed to prevent the server from being filled by a few users. This folder is allocated the drive letter **(H:)**. It is often referred to as “**your H drive**” or “home area”.

Please note that IT Services have administrative privileges and access to your personal folder and all files stored on the school's IT facilities. Please note personal photos or music must not be stored in either personal or departmental folders; it is designed for storing school documents only.

Software

Users of the school's network are not authorised and are unable to load any software onto the IT facilities. Only software licensed to the school may be installed on the school's IT facilities.

Software downloaded from the Internet and/or software obtained illegally must not be loaded onto the school's IT facilities. Any software obtained and/or installed illegally will be reported to the Headteacher.

Remote Access

Remote access is currently only available to selected members of staff that have agreed to the separate Remote Access Services Policy. The use of equipment for remotely accessing the school's network is limited to authorised persons and for school purposes only. When a staff member uses her/his own equipment, they are responsible for the maintenance and repair.

The school bears no responsibility if installation of remote access software, or the use of any remote access systems, causes system lockups, crashes, or complete or partial data loss. The remote access user is solely responsible for backing up all data present on a personal machine before beginning any work. At its discretion, the school will disallow remote access for any user using a personal home computer that proves incapable, for any reason, of not working correctly and securely with the school's provided software.

Any personal home computer used to access the school's remote systems must have installed the same software programs as they are accessing remotely. They must also have installed antivirus and antispyware programs. These antivirus and antispyware programs must be regularly updated (minimum - once a week).

Electronic Communications

Conducting official communications through third party Email accounts (i.e. other than @cardinalallen.co.uk accounts) carries risks of impersonation and other security risks, as well as presenting difficulty in maintaining up-to-date and accurate Email address lists. All staff and students are to conduct official communications with each other exclusively through the school's Email system, with @cardinalallen.co.uk addresses for both sending and receiving.

Students must not attempt to contact any staff member of the school through the use of Facebook or any other social networking site.

Mobile Devices

Mobile devices such as laptops, PDA's and portable storage devices, media and mobile phones pose a particularly high security risk, primarily because they are vulnerable to theft and loss. Their material value is however, of secondary concern when compared to the potential cost of losing or compromising confidential and sensitive data.

Mobile devices are perceived as personal items and are frequently selected, purchased and configured by their end users without consultation from ICT Services. It is the owner's responsibility to ensure that the correct measures have been taken to secure data on mobile devices and have made sure that they are virus free.

The following security controls measure, and guidelines should be taken:

Connection of student owned devices to any part of the school's network is strictly prohibited, unless approved by the Headteacher and IT Services.

Mobile devices should not be left unattended and, where possible, must be physically locked away or secured.

Passwords for school systems must not be stored on mobile devices.

Whenever a device is lost, it must be reported as quickly as possible to the Designated Authority.

The school will not be responsible for restoring data from a mobile device.

Person-Identifiable information must not be stored on a mobile device.

Sensitive data must be encrypted using encryption software.

Password/pin at login must be enabled on each mobile device.

Maintenance & Repairs

It will not be possible to properly support the school's IT Facilities if equipment is not correctly maintained. Any faulty/out of order IT facility should be reported by using the online support desk. Any data stored on faulty IT facilities will be recovered using a "best effort" approach by ICT Service. Any cost incurred by the school in recovering data may be charged back to the user or department involved.

If any IT facilities require external repair, ICT Services will take a "best effort" approach to remove all data ahead of repair.

Copyright and Licence Agreements

Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and learning resources, which they use including software, services documentation and other goods.

Users must not copy or modify any copyright material (3rd party material) nor incorporate any part of the 3rd party material into their own work unless such acts are either permitted under the CDP Act 1988, by a Licence Agreement, or with the permission of the copyright holder.

Users must not install, make, store, or transfer unlicensed copies of any copyright or trademark work including software, videos or music, unless permitted under legislation or with the permission of the copyright holder.

Behaviour

Users must respect the rights of others and should conduct themselves accordingly when using IT facilities to create a beneficial environment for all.

Users must not interfere with or disrupt the availability and use of the IT facilities by others. Users must take every precaution to avoid damage to equipment and learning resources caused by the presence of food and drink in its vicinity. Under no circumstances must food or drink be consumed near any IT facilities.

Infringement

Withdrawal of facilities - If a user is in breach of any of these regulations, the Headteacher may withdraw or restrict the user's use of IT facilities and learning resources, following consultation or in relation to students their form tutor, Head of Year and/or parents.

Removal of Material - The school reserves the right to remove material from its IT facilities without notice where such material is in breach of these regulations.

Disciplinary action - Any breach of the regulations may be dealt with by the Headteacher under the school's formal disciplinary procedure for both students and staff and in some severe cases may result in suspension or dismissal. The user may be charged for any costs that have arisen as the result of misuse or abuse of facilities and/or resources.

Breaches of the law - Where appropriate, suspected breaches of the law may be reported to the police.

Disclaimer

The school accepts no responsibility and expressly excludes liability to the fullest extent permissible by law, for:

The malfunctioning of any IT facility, whether hardware, software or other,
The loss of any data or software or the failure of any security or privacy mechanism.

Staff Guidelines for the Use of Facebook.com - General Practice and Advice

Members of staff must not be in contact with current Cardinal Allen Catholic High School students via social networking sites such as Facebook.com.

Member of staff should also note-

Members of staff with Facebook profiles should set the privacy levels on their accounts to maximum i.e. only people on their friends list should be able to view their pictures/private information etc. This can be done by going to Setting > Profile and adjusting the parameters accordingly.

Members of staff with distinctive surnames should be aware that it will be relatively easy for students to track them down on Facebook.

Members of staff should be aware that having a parent as a Friend will make you easier to find.

Members of staff should note that although these measures will make it harder for students to find them on Facebook, a determined individual with knowledge of how the website works will eventually be able to trace a person down given enough time.

Action to be taken if a member of staff is contacted by a student.

There are two types of contact through Facebook:

1. A message
2. An invitation to be added to a persons «Friends list»

If a message from a student is received, the following action should be taken:

1. Do not reply to the message. Replying to a message allows the recipient to view your profile in its entirety. This is also a way to circumvent the privacy settings on account.
2. A senior member of staff (eg Head Teacher / Designated Senior Person) should be contacted at the earliest opportunity and informed of the incident.
3. Senior member of staff should then be asked to speak to the student on behalf of the member of staff who was contacted. The relevant Facebook correspondence should be made available to the member staff dealing with the situation to aid in any investigation.
4. The student should be reminded of the school's ICT Acceptable Use Policy and that contacting staff in this manner is inappropriate. A note for file and notification to parents should also be made.

If an invitation to a person's friends list is received, the following action should be taken:

1. Immediately reject the invitation.
2. A senior member of staff (eg Head Teacher / Designated Senior Person) should be contacted at the earliest opportunity and informed of the incident.
3. A senior member of staff should then be asked to speak to the student on behalf of the member of staff who was contacted. The relevant Facebook correspondence should be made available to the member of staff dealing with the situation to aid in any investigation.
4. Note that rejection of a «friend request» allows the sender to repeat the action; if this occurs, the relevant members of staff should be made aware of this.
5. The student should be reminded of the school's ICT Acceptable Use Policy and that contacting staff in this manner is inappropriate. A note for file and notification to parents should also be made.

E-Mail – Good Practice

The nature of the Cardinal Allen Catholic High School site, and the busy schedules led by all who work here means that Email can be a vital tool of communication. However, it should not replace the fostering of positive face to face relationships with colleagues. Email should not be regarded as a replacement for formal meetings or more informal conversations on the telephone or at staff briefings, break or lunch. The aim of this brief guide is to provide some suggestions on the way that Email can be used most effectively and to improve the experiences of all those who interact electronically.

Is it necessary?

People are busy. Your message may be one of tens or hundreds for a recipient to deal with depending on how busy they are, how many lessons they have taught that day, how many extra-curricular activities they have been organising. If they are receiving so many messages, what are the chances that they will read your message with great care, particularly if they perceive it to be only tangentially relevant to them? For many people, Email is fast becoming a chore, not a vital tool of communication. Do not accelerate this process by contributing messages / information that could be broadcast or communicated in another, often more efficient, way.

Beware of Forwarding and Replying

Consider carefully the necessity of forwarding a message and to whom. Take great care with any attachments, even from senders well known to you. When forwarding, include a summary of what you are sending – tell the recipients what it is in a sentence or two. If it is worthwhile to forward, it's worth an extra moment of your time to summarise your reason for forwarding it. When replying to an email check that you reply to the intended people only.

Dealing with Emotions

One of the attractions of Email communication is that it can be quick and simple. However, this can also be a weakness. When you are writing letters, the very nature of the activity forces you to think about your choice of language. You may even go through a draft or two – considering carefully the impact of your words on the reader. Emails are often drafted all too rapidly and immediately sent off. Emotions or nuances you may feel were obvious could be missed by the recipient or perhaps they may read into your message and pick up attitudes or meaning that you had no intention of conveying. Humour is notoriously tricky to convey appropriately via Email, even to people that you know well. Therefore, the following suggestions can be useful:

Don't Criticise

Never chastise or criticise someone via an electronic communication. Even well-meaning and constructive criticism can hit home much harder on screen when you are not there to moderate the blow with body language, vocal tone and flexible response to the observed reaction. Even if you do not feel that you are criticising, the perception of a message must always be carefully considered.

Cool Off

If you have something to get off your chest, write the Email message then save it. Let it lie for a few hours / a day, then re-read it. In the meantime, circumstances may change or you may have an opportunity to talk to the person causing your anxiety. Even if little has changed, it is highly likely that you will edit or re-write your original Email and it will be a more effective message for the greater sense

of detachment and objectivity the extra reflection time has provided. Get out of the habit of a quick send then lengthy regret.

Take Care

Before responding to any Email message, re-read it to ensure that you fully understand it. Many messages are sent / forwarded without the reader really grasping the point and responding appropriately. Try to get into the habit of proof reading your own messages. This will ensure that your meaning and your requirements are clear and should help to minimise the chance of misunderstanding or frustratingly irrelevant replies.

Writing the Email

Clear entries in the subject guides to assist the reader in prioritising their inbox and sharp, concise Email messages all play their part in making the process efficient and painless. Avoid putting too much information into one message – your key points may become buried. Email is, by its very nature, designed for short, digestible snippets of information. Readers do not expect tomes and they do not expect additional information beyond the subject guide. If you have lots to say, then it may be lost in a long message – consider breaking it down into several messages or communicating your concerns in a different fashion.

Urgency and Reliability

Email feels immediate. It is not. It is subject to both technical system and reader variables. All staff should try to check their Email twice a day but, as we all know, sometimes this is not possible. Even when it does happen it is most likely to occur at 8a.m., lunchtime or after 4p.m. Bear this in mind when you send a message in the hope of a speedy reply by return. Try the phone. If it is urgent, check staff timetables and seek people out.

Email Conversations

If your Email exchange on one topic results in two or more “cycles”, then it is probably best to stop and talk to each other. Email will simply take too long and the subject is obviously complex enough to need a proper form of exchange with much more interactive feedback.

Email Access and Security

2FA is enabled on all school email accounts to prevent Cyberattacks, phishing and to ensure security. School email can only be accessed in the UK

Summary for Students

This summary has been designed to provide you with the key facts of the ICT Acceptable Use Policy.

Use of IT facilities is forbidden unless supervised by a member of staff.

No passwords are to be spoken, written, emailed, hinted at, shared or otherwise made known to anyone else.

With the exception of portable computers, IT equipment must not be moved, relocated or adjusted without the permission of a member of staff.

Eating and drinking is not allowed in any room with IT facilities.

The use of portable media and portable storage devices, including portable audio players, is forbidden.

Students can only use the email facility in lesson time with the permission of a member of staff.

Connection of any personal devices to the network (wireless or cabled) is forbidden.

Software must not be installed or attempted to be installed onto any computer.

If you accidentally damage or find damaged IT equipment, please report it to a member of staff immediately.

The Internet must only be used for educational purposes.

Use of the school network and the Internet is carefully monitored and recorded.

The storage of personal photos and music on the school's IT network is strictly forbidden.

Messages sent or posted electronically should be polite. Please appreciate that other users might have different views from your own.

Any deliberate attempt to damage or 'hack' into the school's IT network will result in serious disciplinary action.

The playing of non-educational computer games and the downloading of music for personal use is strictly prohibited.

Only the school's email system must be used to send and receive emails in school.

Cyber-bullying

The school regards cyber-bullying, through the inappropriate use of electronic communication such as text messages, Email or postings on social networking websites like Facebook, as an unacceptable form of bullying. This includes the use of technology outside of normal school hours if it interferes with the safety and well-being of any member of the school community. Such incidents will be treated seriously, investigated thoroughly and, if necessary, appropriate disciplinary measures taken

Use of AI

The school promotes the use of AI for both staff and students however personal data must not be uploaded and shared via any online platform (eg Chatgpt). Pupils must be of the legal age to use any AI in school and must be supervised by staff. When using AI resources in school, staff must check that the resources are accurate and suitable for education.

OneDrive Storage

Staff and students must not use portable storage devices in school. Every user account is provided with a school OneDrive that allows users to store documents to the cloud and access on devices outside of school. These files are monitored by the IT Department.

Acknowledgment of ICT Acceptable Use Policy