•

Knowsley Central School

Acceptable Use of IT

Reviewed by:	Michelle McFadden	**Date:**	September 2025
Last reviewed on:	September 2025		
Next review due by:	September 2026(Annually)		

Acceptable use of IT Protocol

There are many benefits to IT but the increased flexibility inherent in the use of IT facilities leads to increased personal responsibility for the user to ensure that the equipment is always used within appropriate guidelines. This Acceptable Use of IT Protocol is designed to reduce the risks and protect you, the school, the Council and its information. The protocol will provide guidance on the appropriate use of the school's / Council's IT facilities, and to provide information on the types of use that may be considered inappropriate.

The protocol applies to all employees of Knowsley Central School and to all other persons working for the Council who have access to, or use of, the Council's IT facilities and equipment, and the term "employee" in this context is intended to include all such persons.

Employees must be aware that noncompliance with the protocol may place the Council's IT infrastructure and the data contained within it at serious risk and may lead to disciplinary action or other equivalent sanction. This may include dismissal or equivalent action where the breach is considered to be sufficiently serious. In certain cases where a criminal offence is suspected, this may be referred for investigation by the police.

GENERAL PRINCIPLES

The general principles apply to ALL aspects of the use of the school's / Council's information technology services. They should be read and understood by all employees using any aspect of the school's / Council's information technology service.

Offensive and/or inappropriate content

As an employee of the school, I understand that I must:

- Notify my manager or the HR service if I receive any form of electronic communication that I consider is, or could be interpreted as, unlawful, offensive or inappropriate;
- Consult my line manager if I am unclear about the appropriateness of any material. As an employee of the school I understand that I must NOT:
- Communicate material (either internally or externally) which is, for example, defamatory, obscene, racist, or which could reasonably be anticipated to be considered inappropriate or offensive

Data Protection and Freedom of Information

As an employee of the school, I understand that:

- Email and other forms of electronic communication may be considered to be recorded information from the Council and could be subject to disclosure to third parties under the Data Protection Act 1998 or the Freedom of Information Act 2000;

- Even if emails are deleted from Council systems, they are recoverable for up to 12 months through IT backups and can be restored for subsequent disclosure and evidence;
- Data stored on local disk drives (C:/ drive) of a PC/laptop are not backed up and may be lost if the hard disk develops a fault

As an employee of the school, I understand that I must:

- Comply with the data protection principles, which include a requirement that computer systems are secure;
- Maintain the same standards of confidentiality when working on material or documents in the workplace or elsewhere (including at home);
- By default, save all data (including word documents and spreadsheets) to the appropriate fileserver;
- Only use encrypted portable storage devices (including laptops)
- Ensure that any electronic data authorised to be shared with a third party is undertaken in a secure manner approved by the IT Service

As an employee of the school I understand that I must NOT:

- Store data on unencrypted portable / removable storage devices (inc. laptops, USB drives etc.);
- Allow third parties to access any school / council information without confirming that they are authorised to have such access

IT Equipment

As an employee of the school I understand that:

- All IT equipment purchased by the school remains the property of the Council until it is formally written off and the IT Service informed

As an employee of the school, I understand that I must:

- Recognise that the equipment loaned to me specifically to support my work in the school is of high value, highly desirable, extremely portable and vulnerable to theft
- Take all reasonable precautions to use the equipment in an appropriate manner and prevent damage / loss occurring (e.g., not leaving any IT equipment unattended in a car)
- Provide a regular visual check of all IT equipment on loan when requested by a member of the SLT
- Arrange all movements and redeployment of IT through the Business Manager
- Notify the Business manager and the IT Service Desk immediately if any IT equipment is lost or stolen;
- Return IT equipment to my line manager or the IT Service immediately upon request

As an employee of the school, I understand that I must NOT:

- Connect any non-Council owned device to the Council's IT network without prior written authorisation from the Head of Information Technology (this includes devices owned by consultants, contractors and suppliers)

Virus Transmission

As an employee of the school, I understand that I must:

- Report any suspicious messages and/or files to the IT Service Desk

As an employee of the school, I understand that I must NOT:

- Attempt to change any administration settings on computers that I use
  Transmit by any electronic means any message, file or attachments which I know or suspect to be infected with a virus;
- Download any software (Inc. Screensavers) without the prior written approval of the IT department
- Forward virus warnings (unless requested to do so by the IT Service Desk)

Copyright

As an employee of the school, I understand that I must:

- Ensure that any material used from the Internet or other sources complies with copyright and other relevant legislation;

As an employee of the school, I understand that I must NOT:

- Use the school's IT facilities for unauthorised copying or retransmission of recordings from whatever media [including CD and DVD] that may infringe copyright

Breach of Confidence

As material can be easily forwarded and copied by the use of IT facilities, a breach of confidence may be more likely to arise.

As an employee of the school / Council I understand that I must:

- Have in mind the Council's Code of Conduct for all employees when using IT services, in particular when dealing with confidential information or using it for any form of communication;
- Seek guidance from my line manager or head of service if I have any doubts about the use, sharing or transmission of confidential information

As an employee of the Council, I understand that I must NOT:

- Supply the Council's bank details to any person or organisation without prior written authorisation from the Borough Treasurer. This includes all aspects of ecommerce

Contractual Relations

Provided that an external party reasonably believes that an employee has the authority to negotiate, or enter into, an agreement, then the school will be bound by the employee's actions. Emails and other electronic communication made by employees can be acknowledged as originating from the school; therefore, recipients will in most cases be acting reasonably if they assume that they are sent with the school's authority.

As an employee of the school, I understand that I must:

- Exercise care when using electronic communication with external parties;
- Ensure that I am authorised to enter into any actual or implied contractual agreement

Obscene Material

As an employee of the school, I understand that:

- The publication of obscene material is a criminal offence; the definition of "publication" includes electronic storage or transmission of material and therefore, I must not publish such material

Personal Use

As an employee of the school, I understand that I must:

- Only use school IT equipment for personal matters in my own time;
- Consider the volume of personal files stored on local drives; in particular media files - 1 Gigabyte of disk space is deemed an appropriate limit for personal files;
- Comply with copyright, data protection and other relevant legislation if using School IT equipment for personal matters

As an employee of the school I understand that I must NOT:

- Store excessive amounts of personal files on any school computer (i.e. more than 1Gb);
- Store any personal files on the school's fileserver's;
- Undertake any actions on school IT equipment which may bring the school's name into disrepute

Private or Third-Party Business Use

As an employee of the school, I understand that I must NOT:

- Under any circumstances use school IT facilities in relation to any private or third party business;
- Use school IT facilities in relation to personal work with charities (e.g. youth organisations) without prior approval from my line manager

Email

Business Use:

The provision of email is predominately for use in association with the school's business; therefore, all use must conform to agreed standards and security requirements.

As an employee of the school, I understand that I must:

- Understand the general principles for the use of IT;
- Comply with the 'use of email - guidance for employees'

- Consider the legal considerations, outlined in the general principles (above), prior to sending emails;
- Use officially provided email addresses to send all business-related emails. Officially provided email addresses include "@knowsley.gov.uk", "@knowsley.gcsx.gov.uk" and "@staff.cfl.klear.org.uk";
- Use secure email solutions (e.g. GCSx, GJSM and CRES) when sending emails that contain personal, sensitive or confidential information outside of the Council's secure email service;
- Comply with the Data Protection Act) for any data being transferred, especially when transfer is outside of the European Economic Area (EEA);
- Ensure that all recipients of an email are entitled/authorised to view the contents;
- Seek advice from my line manager, head of service, the HR Service or the IT Service if I have any queries about business use of email

- As an employee of the school, I understand that I must NOT:
- Send or forward business emails or electronic files of any sort to my home email address;
- Send emails to people if I am unsure if they are entitled/authorised to see the content;
- Use council email facilities for the transmission of unsolicited commercial or advertising material, chain mail or other junk-mail of any kind to colleagues or any other organisation;
- Create or transmit anonymous messages, i.e. without clear identification of the sender;
- Create or transmit material which could bring the school, Council or its partners into disrepute;
- Send emails to large distribution groups without the authorisation of my head of service;
- Send emails with large attachments without a legitimate business reason (5Mb is classed as large)

Personal Use

The school recognises that there may be a small number of occasions where staff may wish to use email for personal correspondence. This is permitted, on occasion.

As an employee of the school, I understand that:

- Personal emails are subject to the same monitoring as business emails and are recoverable for up to 12 months after deletion through IT backup systems

- As an employee of the school, I understand that I must:
- Undertake personal use in my own time;
- Ensure that such use is lawful and complies with the Council's other policies;
- Ensure that personal use does not have a negative impact on the school, the Council or its partners;
- Add the following disclaimer to all personal emails sent from Council email facilities:
- "This email is personal. It is not authorised by, or sent on behalf of, Knowsley MBC. This email is the personal responsibility of the sender."

- As an employee of the school, I understand that I must NOT:
- Allow email use to interfere with performance or priorities of my or another person's duties;
- Conduct any form of private or third-party business using the Council's email service;
- Send excessive emails or large attachments;
- Use business email addresses to register for personal websites (for example banks and online shopping), personal use of social networking sites or to confirm orders for personal goods or services;
- Use secure email services (e.g., GCSx and CRES) to send personal emails

Mailbox Management

To ensure that emails can be received and sent efficiently it is important that some basic email management processes are adopted.

- As an employee of the council, I understand that I must:
- Use the standard “out of office‟ function when I am unable to access my email for more than 24 hours, excluding weekends and bank holidays.
- “Thank you for your email. I am currently out of the office until [insert date]. I will respond to all emails upon my return. If the matter is urgent, please contact [insert name and contact details of colleague or team to be contacted in your absence.]”
- Archive old emails and calendar appointments and keep mailboxes within agreed size limits; ‟
- Refer to the specimen retention schedule or management retention schedule when archiving old emails and calendar appointments
- Delete transitory and non-council emails as soon as possible after the email has been sent and/or received

- As an employee of the council, I understand that I must NOT:
- Grant delegate access to my mailbox to anyone who does not have a legitimate business need to view all content that maybe received to it or contained within it;
- Exceed agreed mailbox limits as this may prevent the future receipt of emails and/or sending of emails

- **All Internet Use**

- As an employee of the Council, I understand that:
- All Internet use is monitored and recorded by date, time and websites accessed;
- Filtering software is also used to protect the Council's information technology network, data and reputation;
- Attempts to access restricted sites will lead to a 'red hand' screen being displayed, a record will be made of the event and that all such occurrences must be reported;
- Attempts to access Internet sites that may constitute a security threat or sites that have not been assigned a category will be blocked by either a “blue hand” or “green hand” screen which requires no further action;

- My Internet access will be identified in the outside world as having originated from the Council, and therefore inappropriate use may bring the Council or its partners into disrepute.

As an employee of the Council, I understand that I must:

- Report all occurrences of a “red hand” screen to my line manager immediately;
- Gain prior written approval from the Head of Information Technology if there is a legitimate reason (e.g., IT support/audit) to breach any of the “must NOT” parameters below;
- Seek authorisation from the Corporate Communications Manager before I subscribe to, enter or utilise social networking sites in relation to any role in the school

As an employee of the council, I understand that I must NOT:

- Knowingly attempt to access an Internet site that may contain pornography or other
- “unsuitable” material that might be deemed illegal, obscene or offensive;
- Create, download or upload material that contain pornography, illegal or other "unsuitable" material that might be deemed illegal, obscene or offensive;
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video, computer programs or image files;
- Subscribe to, enter or use online gaming or betting sites;
- Subscribe to or enter "money making" sites or enter or use "money making" programs;
- Use Council Internet facilities to run a private business;
- Download any software without the prior written consent of the Head of Information Technology;
- Stream live sports events or concerts as this can present a security risk and impact on network performance;
- Watch live television broadcasts via the Internet unless the building I am in has a valid TV Licence and I have been authorised to watch such broadcasts for business purposes.

Personal Usage

The school recognises that there may be a small number of occasions where staff may wish to use the Internet for personal purposes. This is permitted, on occasion.

As an employee of the school, I understand that:

- All Internet use is monitored and recorded by date, time and websites accessed;
- Filtering of Internet sites applies to all use, including personal use;
- The school is not responsible for any personal transactions that I enter into (for example in respect of the quality, delivery or loss of items ordered);
- All personal usage must be in accordance with relevant policies;
- My computer and any data held on it are the property of KCPSC / Knowsley MBC and may be accessed at any time by the school / Council to ensure compliance with all its statutory, regulatory and internal policy requirements

As an employee of the Council, I understand that I must:

- Undertake personal use in my own time;
- Ensure that such use is lawful and complies with the school's and Council's other policies;
- Ensure that personal use does not have a negative impact on the school, Council or its partners;
- Keep the school /Council protected against, any claims, damages, losses or the like of which might arise from any transaction;
- Seek advice from my manager if I am in any doubt about how I should use the Internet for personal purposes

As an employee of the school, I understand that I must NOT:

- Allow personal Internet use to interfere with performance or priorities of my or another person's duties;
- Use Council Internet services to conduct any form of work for a third party or private business regardless of whether it is for reward or not;
- Imply in any way that I am acting on behalf of the school / Council;
- Use business email addresses to register for personal websites (for example banks and online shopping), personal use of social networking sites or to confirm orders for personal goods and services;
- Use a business address to support personal orders or as the delivery address for online orders

All Intranet

As an employee of the Council, I understand that:

- All Internet use (including access to BERTHA) is monitored and recorded by date, time and site accessed;
- BERTHA is provided primarily for business related purposes for all PC based council staff;
- Any information stored or provided on BERTHA (including information on My Sites / Team sites) is intend solely for internal circulation within the council
- Any non-business-related features provided via BERTHA are intended for staff to take advantage of within breaks or their own time

As an employee of the Council, I understand that I must:

- Use BERTHA primarily for business related purposes;
- Comply with information management and security policies and guidance and ensure that information is only shared with authorised colleagues;
- Ensure that personal use of BERTHA does not have a negative impact on the productivity of the Council or its partners;
- Comply with the 'personal use' guidance above

As an employee of the Council, I understand that I must NOT:

- Allow use of non-work related features of BERTHA to interfere with performance or priorities of my duties;
- Share or pass on information from BERTHA to external parties outside of the council

- Store any personal multimedia content (photographs, music etc) anywhere on BERTHA or SharePoint

Acquisition/Installation /Use

As an employee of the Council, I understand that I must:

- Obtain approval from the IT Service for all software that is purchased and/or installed on school computers;
- Purchase all software through approved suppliers;
- Ensure that I have a valid and appropriate licence for all software that I use;
- Register all software in the name of Knowsley Central School (Knowsley MBC) and not an individual;
- Pass all software source materials (CDs, tapes etc) to the IT Co-ordinator (Service) for safe storage;
- Report any suspected software misuse to the Head of Information Technology

As an employee of the school, I understand that I must NOT:

- Download any software from the Internet (including Google applications, iTunes etc) other than for school use;
- Install any software from any source without the written consent of the IT Technician or Head of Information technology (this includes evaluation and shareware software);
- Use any personal software on a school computer;
- Make copies of any software licensed to the school / Council;
- Use any software purchased by the Council on any non-Council computer;
- Develop any software applications (including MS-Access) without the prior written approval of the Head of Information Technology

Removable Media

The Data Protection Act (1998) requires that the Council has appropriate technical and organisational measures in place to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Removable media can hamper compliance with the Act and place information at risk.

Removable media devices include, but are not restricted to the following: CDs; DVD's; Optical Disks; External Hard Drives; Media Card Readers; USB Memory Sticks (also known as pen drives or flash drives); Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards); MP 3 / video Players (inc. iPods); Digital Cameras.

All Use of Removable Media

- As an employee of the Council, I understand that I must:
- Comply with the data Protection Act when transferring data to removable media and seek appropriate advice if required;
- Have written authorisation from the Information Asset Owner (service director or head of service) before I copy any Council data/information onto removable media;

- Use encrypted devices for all data/information which has been authorised for transferred to removable media;
- Seek approval from my line manager and the information asset owner prior to burning any data on to CDs/DVD's using permitted computers
- Keep removable media devices securely;
- Report the loss of any removable media device containing school data to the IT Service and my line manager as soon as I become aware of the loss;
- Return removable media devices containing school data for cleansing if I leave the council or if I am requested to return them at any time;
- Delete all personal/sensitive/confidential information from all unencrypted removable devices - seeking advice from the IT Service if necessary;
- Seek advice from the Council's Corporate Records Manager if I have any queries

As an employee of the Council I understand that I must NOT:

- Transfer any Council data to an unencrypted removable device

Failure to Comply

Failure to comply with any element of this guidance will result in the Disciplinary process being instigated.

Information Security

The Council recognises the importance of information as an asset and the need for proper, effective management of information held on all systems. It is essential that;

- We have proper access to information which will assist in the delivery of the school's services but we must also be certain that we only retain information we need
- We up hold the individual's right to privacy
- We disclose personal data on request to that person under the Data Protection Act
- On request supply to the public information, we hold under the Freedom of Information Act subject to certain statutory exemptions
- There are security safeguards to ensure the continuous availability, integrity and confidentiality of all our information systems

We will;

- Only use or access information and information systems for business purposes and ensure it is always accurate, complete and up to date
- Retain all files required for the purpose of disclosure but only disclose and share information with those authorised to receive it
- Ensure that all employees take personal responsibility for the management of their information
- Ensure effective systems are in place to manage the retention of relevant information and the removal of unnecessary data

The Policy applies to all the employees directly or indirectly managed who are involved with delivering council services and/or which have access to council information in whatever capacity including:

- Elected Members
- Permanent employees of the council or an affiliate organisation, Individuals contracted by the council through the council's contracted suppliers for agency workers/consultants,
- Employees of sub-contractors of the council,
- Any other individuals with authorised access to Council information assets or information processing facilities

Failure to Comply

- Relevant sections of the policy may be used as a reference point in specifying contracts with external suppliers.
- The Security Policy applies to all premises, physical equipment, software, and information owned or managed by the council, directly or indirectly through subcontractors, to deliver services.
- This scope notably includes information relating to authorised users that is stored or processed.