Appendix A: Internet and Email Acceptable Use Policy

Scope

The following policy relates to all Lancashire County Council Members and Co-opted members who capture, create, store, use, share and dispose of information on behalf of Lancashire County Council.

These persons shall be referred to as "Councillors" throughout the rest of this policy.

Lancashire County Council shall be referred to as 'the council' or 'we' throughout the rest of this policy.

Purpose

The council will provide internet, email, telephone and collaboration tool facilities to Councillors where they are required to carry out council duties. To ensure security and compliance with council policies, councillors must only use LCC provided systems or equipment for council business.

This policy outlines the acceptable use of email, telephony, Microsoft Teams, and any other communication or collaboration tools provided by the Council to ensure secure and efficient communication where they are required to carry out council duties. These tools must not be used in ways that the council considers to be unacceptable.

The Council has a suite of Information Governance Policies that apply to all users, including Elected Members which can be accessed on the LCC intranet.

Monitoring

For security purposes, all processes and actions carried out on a corporate laptop or desktop computer are monitored and the data stored and analysed by the corporate security system. This data is held within Microsoft 365 for a minimum of 30 days and then automatically deleted.

The council can monitor use of internet, email, telephone, and Microsoft Teams facilities and examine records without informing individual users.

The council regards all messages and transmissions using these facilities as the council's property and responsibility.

Councillors cannot assume that private transmissions will be private.

When monitoring communications, such as emails, that are clearly marked personal the council will avoid, wherever possible, opening those messages.

Councillors must be aware that all messages and transmissions using council facilities can and may be monitored in full by the council to enforce the council's policies and codes of conduct.

The council will not consider comments contained in emails or posted to any other system visible on the internet as formal statements issued by, or the official position of, the council and Councillors should not phrase them as such. A disclaimer appears on all outgoing emails.

Council rules and conventions which govern expressions of opinions about the council or council business in public areas continue to apply if you use social media sites (such as Facebook) in your personal capacity.

Councillors who use social media platforms should also refer to the social media protocol at Appendix 'B'.

This policy should be read in conjunction with other Information Governance Policies, Additional Protocols and the Code of Member Conduct.

Permitted Use

Although the council permits some non-council business use of corporate communications tools, all personal use of these facilities remains subject to acceptable use rules relating to purposes and content (see below).

The use of corporate communication tools for the purpose of contact with personal representatives and for essential communication with home for co-ordinating council business and family life are within the definition of 'council business use' and are therefore acceptable.

The council also restricts access to systems such as email and MS Teams from outside the UK and Ireland. However, due to the need for Councillors to continue working from destinations outside the UK and Ireland, councillors can request for access to be enabled for a specified period while traveling abroad. Not all countries are on the "approved list" of countries to request access for, and any request to gain access to a country not on the approved list would be considered on a case-by-case basis.

Acceptable Use

Email

Councillors must:

- always use their county council provided email address for county council business, except in emergency situations.

- Avoid sending external emails containing personal or sensitive information, unless the email is encrypted, or a secure private link is in place.

- Refer to the Email encryption guidance provided by Digital Services.

For a list of external organisations with whom there is a secure private link in place refer to Digital Services article KB0019211.

- Ensure all communications are respectful, professional and comply with the council's Communications Guidance and Email signature and Guidance.

- Check all email correspondence before you send it to ensure that the recipient details and any attachments or links to documents are correct.

Please note that Councillors can access further technical support from Digital Services by telephoning 01772 532626 and pressing 'option 4'.

Guidance on Handling Different Information Formats Electronic Information

Email

Corporate email addresses must be used for professional communications.

Individual users are responsible for the emails that they send and should take all necessary precautions to ensure that the recipients listed in their email are the correct recipients. Disclosures of personal, sensitive or confidential information to incorrect recipients must be reported as an information security incident.

Care should be taken to ensure that any attachments to emails are those intended to be sent with the communication.

Appropriate labelling of documentation will assist users and reduce errors from occurring.

Users must not send personal, sensitive or confidential information to their home email to work on.

Users must avoid sending external emails containing personal or sensitive information, unless the email is encrypted. Refer to the Email encryption guidance provided by Digital Services. For a list of external organisations with whom there is a secure private link in place refer to Digital Services article KB0019211.

Bulk emails should be sent with recipients 'blind copied' (bcc) to prevent the disclosure of personal contact data to other recipients. The council's Communications Team manages a corporate mailer application specifically designed for sending 'bulk' emails such as newsletters.

Users must check all email correspondence before sending to ensure that the recipient details and any attachments or links to documents are correct.

Ensure all communications are respectful, professional and comply with the council's Communications Guidance and Email signature and Guidance.

Microsoft 365

Microsoft Teams should be used for business calls, video conferencing, collaboration and meetings.

All users must complete Information Governance e-Learning and read the Acceptable Use Policy: Internet, Email, Telephony, Communication and Collaboration Tools.

Users are responsible for verifying that individuals invited into Teams calls are from a genuine and trusted source and that invitations are sent to the correct email recipients. Users must ensure that any invitations inviting them into external Teams calls are from a genuine and trusted source.

Call participants must be informed in advance and agree to the recording of any Teams calls. Recorded content must be held securely and may be subject to disclosure under the access provisions of UK GDPR/DPA 2018, FOIA (2000) and EIR (2004).

Users are responsible for ensuring the confidentiality and security of all data processed within Microsoft 365. Only the minimum required amount of personal, special category, or sensitive data should be disclosed where a lawful basis exists.

Users must manage external access to Microsoft 365 in accordance with the council's Information Governance Policies.

Users must ensure meetings and video conferencing within Microsoft Teams are conducted appropriately, maintaining data security and confidentiality. Users should refer to further guidance on keeping information secure.

Generative AI Tools

The council's corporate GenAI tool, Copilot helps automate processes, improve efficiency in repetitive tasks, and analyse large data sets quickly.

Before using authorised GenAI tools, users must read the GenAI Policy and ensure that use of Gen AI tools adheres to data protection laws and all organisational policies.

Users must not:

- Use unauthorised GenAI tools to write letters containing personal details.
- Upload customer data spreadsheets for GenAI analysis.
- Use any unauthorised GenAI products other than those approved by the council.
- Use GenAI apps on personal phones to record and summarise work meetings, or to use translation services.

- Use an external or free GenAI tool downloaded to a personal phone and input personal or sensitive council data is not authorised and could constitute a data breach.

If users have any doubt about the confidentiality of information or what will happen to the data they enter, they should not use that GenAI tool.

Information Security

Councillors must follow guidelines on keeping information secure and be aware of your working environment and surroundings at all times, including if you are working agilely or from home.

Hardcopy Documentation

Councillors should avoid printing documentation unless absolutely necessary. Any remote, agile or 'home' printing must adhere to Information Governance Policies and the Councillor home printing and scanning guidance.

Documentation in hardcopy format must be handled strictly in accordance with this policy and the Information Handling Policy and disposed of using 'Confidential Waste' bins which are available throughout council buildings.

Mobile Devices

The council does not permit the use of corporate mobile phones whilst driving unless using an appropriate hands-free kit.

Only council supplied SIM cards should be used in council supplied devices.

Acceptable Business Use:

For councillors, "Council Business" means business relating to the work of the Council or Councillors, and includes:

- Dealing with correspondence from members of the public on constituency business.
- Correspondence with officers of the council on matters relating to the business and operation of the council.
- Political Group business.
- Subscribing to newsletters relating to the work of Councillors or Councils.
- Frequenting chatrooms, discussion forums etc relating to the work of Councillors or Councils.
- Use which facilitates the operation of the business of the county council.

See Appendix 'B' on the use of social media.

Unacceptable Uses and Purposes

The council defines unacceptable uses, purposes, and frequent non-council business use as follows. This list is not exhaustive:

Unacceptable Uses:

- Any illegal activity, breach of council policy, or actions against the council's best interests.
- Non-council business use for unacceptable purposes.
- Frequent or time-consuming non-council business use of internet, email, telephone, Teams, or other communications systems.
- Content that is inappropriate or unauthorised disclosure of council or customer information.

Unacceptable Purposes:

- Running a private business, whether for profit or not.
- Private business or financial transactions, including gambling and shopping.
- Computer crimes such as hacking.
- Harassment of any kind.
- Downloading, streaming or storing of music and/or films.
- Any use of internet facilities, which would allow the concealing non-council business use of council systems.
- Accessing sites that are blocked for reasons of legality or taste without approval.
- Using your council email address for non-council business use.

Examples of Non-Council Business Use:

- Using council email for non-council newsletters or services.
- Using council email as a contact for personal websites.
- Social media activities unrelated to council business.
- Uploading personal photos or information to websites such as Flickr and Wikipedia.
- Online auction activities for example, eBay transactions.
- Creating publications for sale, or personal websites and blogs.
- Participating in non-council business related chat rooms, discussion forums, or personal messenger services.
- Non-council business related peer to peer exchanges.

Frequent Non-Council Business Use:

- Excessive visits to sports or news sites.
- Personal distribution lists with more than five addresses.
- Bulk personal emails.
- Participating in chain letters or petitions.

- Sending large attachments in non-council business emails.
- Excessive chatting or distributing jokes.

Unacceptable Content

Certain types of content are deemed unacceptable and may be accessed or copied from websites, or contained in emails and messages as text, graphics, or sound. These include:

- Content that brings the council into disrepute.
- Content that infringes copyright.
- Content that could be reasonably construed as discriminatory, offensive, defamatory, or obscene.
- Content that is derogatory about an individual’s race, age, disability, religion, national or ethnic origin, physical attributes, or sexual life.
- Content containing abusive, profane, or offensive language.
- Content that contradicts the council’s values of respect for all, promoting shared values, and fostering safer communities, such as content promoting hate incidents or hate crimes.
- Content that engages in or promotes extremist activities or views.

The Counter-Terrorism and Border Security Act (2019) creates additional powers and provisions in relation to terrorism and creates new offences in relation to terrorism, which include the offence of the reckless expression of support for a proscribed organisation , the offence of the publication of images or seizure of articles and the offence of obtaining or viewing terrorist material over the internet.

Review and Updates

This policy will be reviewed annually by the Corporate Information Governance Group (CIGG) and updated as necessary.

Contact

Email: DPO@lancashire.gov.uk

Version Control

Title	
Document author(s) name and role title	Joanne Winston, Information Governance Manager
Document owner name and role title	Heloise MacAndrew (SIRO)

Date of creation	January 2025	**Review cycle**	Annual
Last review		**Next review date**	January 2026