IA

Information Security and Acceptable Use Policy

Contents

1. Introduction

We must take the utmost care over the information and data we hold and the way in which it is used to ensure it is managed and looked after properly. Our customers expect us to safeguard their information always. The simplest mistakes can have serious outcomes for the people they affect.

Electronic communication tools are important to Leicestershire County Council and support elected members, staff and individuals/organisations working on our behalf to deliver services to the public. However, inappropriate use or abuse of information and data resources (both electronic & physical hard copies) can put the council, its employees, elected members and service users at risk and could incur a fine or sanction from the Information Commissioner's Office. We have a legal duty to protect personal and/or sensitive information and data.

Supporting documents, the exception process and more detailed guidance around this policy are available on the intranet.

Back to Contents

Scope

This policy applies to:

All forms of information and data owned, administered, stored or controlled by the council, including electronic and hard copy formats;

All elected members and staff of the council including temporary and contracted staff, volunteers and third-party contractors accessing or using the council's information, data and/or network; and

- All electronic and communication devices owned, administered, controlled or sanctioned for use by the council.

Back to Content

2. Equalities

The council's commitment to equality of opportunity will be observed at all times during the operation of this policy. This will ensure that employees are treated fairly and without discrimination on the grounds of race, nationality, ethnic or national origins, sex, marital status or civil partnership, disability, age, sexual orientation, trade union membership or activity, political or religious belief, maternity or pregnancy, gender re-assignment and unrelated criminal conviction.

Back to Contents

3. Policy Statement

Leicestershire County Council entrusts the individuals/parties identified in section 2 above to use the council's information, data and IT facilities sensibly, professionally, lawfully, consistently and in accordance with this policy and the council's rules, procedures and contractual arrangements.

Any inappropriate use of the council's information, data or communications systems whether under this policy or otherwise could constitute gross misconduct and may lead to disciplinary action up to and including summary dismissal for staff and may give rise to a breach of the code of conduct for elected members.

This policy sets out clear rules for the use of the council's information and data with its communication systems, networks, software and tools.

Back to Contents

4. Duties and Responsibilities

Some staff have specific responsibilities for information security and data protection e.g. the Senior Information Risk Officer (SIRO), the Data Protection Officer (DPO), Caldicott Guardians and Information Asset Owners. Details of their and other officers responsibilities are available in the Information and Data Governance Policy.

Some responsibilities apply to everyone. As an employee, individual or elected member working for, or on behalf of Leicestershire County Council it is essential that you understand and abide by the following rules.

4.1 Inappropriate Use

It is strictly prohibited to use the council's resources to create, download, store, access or transmit any:

- Defamatory, obscene, offensive or otherwise unlawful images, data or information

Material that is designed to annoy, harass or cause needless anxiety to other people, as detailed in the "Employee guide code of conduct"

- Material that violates copyright law
- Material for the purpose of corrupting or destroying the council's network or data
- Junk mail or spam

Never impersonate another person when using email or amend any message received.

The authority uses website and email filtering software, so you will not be able to access certain sites or send e-mails containing certain words.

4.2 Personal Use

The council allows staff some personal use of the web, internal (but not external) email and limited occasional use of a work phone, but you must still abide by section 5.1

However, as staff, you must not access the web or send personal emails during work-time, i.e. personal use should be before or after work or at lunchtime/breaks. Any personal use must not be to the detriment of, or interfere with, your work or the work of others. Access to personal email accounts is not permitted. Personal use of the council's facilities must not incur unwarranted expense for the organisation. Leicestershire County Council reserves the right to monitor personal use of the council's facilities.

4.3 Working with Council Information

Individuals working for, or on behalf of Leicestershire County Council, including elected members, must ensure that the information and data they are accessing and using is managed and processed lawfully, fairly and in a transparent manner. This means you must:

- Only use personally identifiable information and data if there is a clear business reason to do so
- Never attempt to modify any data, information, systems and equipment without appropriate authorisation
- Ensure there is proper consideration of the potential risks and possible impact of using personal, special (sensitive) and confidential information for your work
- Only access personal records/data for work purposes. You must not look up or alter your record or the records of friends, family or acquaintances unless specifically authorised. Any conflict of interest (or potential conflict) must be brought to the attention of your line manager
- Take care to ensure that personal, special (sensitive) or confidential information is not released/shared without appropriate authorisation and/or agreement and secure methods are used to transfer information (See Information Sharing on the Intranet)
- Ensure when sending information, that you have the correct address and recipients name
- Only print personal, sensitive or confidential data and information when necessary and store or destroy the information in a secure manner
- Not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised
- Abide by any physical security measures in place on council premises e.g. wearing your ID badge, and not allowing others access using your badge
- Abide by the council's clear desk policy and not leave personal or special information unattended on desks when you are away from them. Personal, special and confidential information should be locked away overnight.

4.4 Use of Email

How you communicate with people not only reflects on yourself but also on Leicestershire County Council as an organisation. Comments and opinions made in emails can be misinterpreted. Electronic messages are accessible to the public under the Freedom of Information Act (2000) or to service users under the UK GDPR and the Data Protection Act (2018) and can be used as evidence in court. If you are conducting council business, you must:

- Use the council's email service
- Input the correct email address
- Not auto-forward to an external email address and manager's must not auto-forward to their team
- Not forward an email string to others if it will mean releasing personal, special (sensitive) or confidential information without relevant authorisation and don't forward it to your personal email account
- Ensure that when you send special or confidential information via email, you use an approved secure method and the email is encrypted
- Emails are council records just like any other documents. Therefore, they should be filed in the appropriate part of your file plan and retained and disposed of in line with the schedule agreed in the Record of Processing Activity (ROPA).

4.5 Social Media

Social media is the term commonly given to websites and online tools that allow users to interact with each other in some way - by sharing information, opinions, knowledge and/or interests.

The following examples of social media are not an exhaustive list: Facebook, LinkedIn, Google+, Twitter, Tumblr, YouTube, Vimeo, Flickr, Instagram, Snapchat, WhatsApp, Yammer Discussion forums

If you are using social media to conduct council business, you must:

- Take effective precautions to ensure your own and others safety is protected
- Only comment on areas of work that are within your responsibility
- Deal with information appropriately. Personal, special (sensitive) and confidential information must not be shared via social media
- Appropriate permissions must be obtained before using or sharing photos on social media

The council's Communications Unit is responsible for using social media on behalf of the council. Any other use of social media by staff for council business **must be approved in advance** by the corporate Communications Unit.

If approved, you will be expected to follow guidance from the Communications Unit. Caution must be exercised when using social media for work purposes, particularly when responding to potentially contentious posts. Further advice is available from the Communications Unit, but in general you are expected to maintain the same high standards of conduct and behaviour as would be expected elsewhere.

Staff using social media for personal purposes, are solely responsible for the content they publish or associate with. Staff should be mindful that content published on social media sites cannot be considered private even if it is shared in a forum with restricted access (such as on someone's Facebook wall or a private group).

Any content published (or associated with) by staff on personal social media accounts deemed to be inappropriate i.e. could undermine their own and/or the council's reputation and/or bring the council into disrepute; will be investigated via the Disciplinary Policy and Procedure and could constitute gross misconduct and may lead to the member of staff's dismissal from the council.

Instances of "cyber bullying" against fellow staff will be investigated under the "Behaviour in the Workplace Policy" and may result in the member of staff's dismissal from the council.

Staff should never provide comment or opinion about Leicestershire County Council, its people or service or ex-service users or their relatives or our partner organisations and suppliers

Elected Members should consult Members Secretariat or read the Advisory Note on Social Media.

More guidance is available on the Intranet.

4.6 Smarter Working

When you are working on council business away from council premises including shared offices, touchdown points, clients' houses or at your home, it is critical that you safeguard the security of any council information, data, systems or equipment you may need to access and/or use. You must:

- Keep all personal and/or special (sensitive) information and equipment containing it safe and stored in a secure cabinet/cupboard if possible
- Store and transfer council information on appropriately secured or encrypted council servers, systems and equipment. If you need to use a laptop or mobile device offline, you must move any saved work into the appropriate location on the council's network as quickly as possible and delete any temporarily saved information
- If your department allows work use of memory sticks, only use encrypted memory sticks that have been provided by Information & Technology Services. Elected Members should consult staff in Members Secretariat
- Ensure your work cannot be viewed by any other person unless authorised
- Only use the council's information and equipment when it is safe to do so
- Never store council information, laptops and other mobile devices (e.g. memory sticks) in an unattended vehicle unless authorised
- When discussing special (sensitive) information consider who is around you and who might overhear – where possible be discreet and don't allow subjects of the conversation to be identifiable
- Only use council approved methods for 'Remote Access' to the council's network and data

4.7 Network, Systems & Equipment Security

The council's IT network, systems and electronic communications equipment are designed and managed to support the organisation and its people to deliver public services. They are primarily for business use and when using them, you must:

- Never attach any equipment (including personal devices, network equipment and any equipment that has been attached to another network) to the council's computer network unless it has been checked and approved by Information and Technology Services. This is necessary to reduce the risk of virus attacks
- Ensure that all in-bound and out-bound connections to council equipment from external networks follow the council's network security arrangements
- Never interfere with the configuration of any electronic communications devices without the approval of Information and Technology Services
- Only use licensed software and apps on council computers, servers and communication devices. Software and hardware should only be approved and installed by I&T staff.
- Only use cloud-based services (e.g. SAAS, IAAS) that have been assessed and approved by I&T Services
- Never impersonate another person or seek to gain access to the council's network, systems, information and data if you are not authorised to do so
- Never share or leave on display any passwords/PINs you need to access the council's network and systems. Supervise anyone using your PC etc. while you are logged-on.
- If you become aware that someone knows your password - change it immediately e.g. if I&T staff need your password/PIN/code to upgrade software on your work device.

- Always lock your computer or mobile device when you are away from your desk and ensure that any hard copy information is stored safely

Back to Content

5. Inappropriate Use and Security Breaches

All breaches and suspected breaches of this policy **must be reported**, via your line manager, your department's Information and Technology Business Partner, the I&T Service Desk or direct to the Information Governance Team. Actions or neglect leading to a breach of this policy, or failure to report a breach will be investigated.

If council information and equipment (e.g. laptops, mobile devices, case files and paper records) you use to do you work is lost or stolen, you must tell your manager as soon as possible. If a laptop, mobile device or piece of equipment is lost or stolen when you are not on council premises you must also inform the police.

In the case of elected members all breaches, suspected breaches or any loss of council information or equipment must be reported to Members Secretariat.

Back to Contents

6. Monitoring

Leicestershire County Council will respect your privacy and autonomy in business communications. However, in certain circumstances it may be necessary to access and record business communications for the council's business purposes.

Leicestershire County Council systems including all related equipment and applications (including internet access) is provided only for authorised and acceptable use as defined by this Policy. All activity and information placed on or sent over these systems is monitored. Logs created as part of this monitoring may be used to investigate suspected unauthorised use or breach of this policy and may lead to administrative, disciplinary or criminal action.

However, website and e-mail filtering software automatically check URLs and scans emails. This could result in websites and e-mails being blocked. Any blocked e-mails will then be checked manually. More information about monitoring is available on the Intranet.

Back to Contents