IT & ACCEPTABLE USE POLICY

Version: 1.0
Adopted: 12th March 2026
Next review: March 2029

1. Introduction

This policy sets out how Caistor Town Council manages information technology, digital working and information security in a proportionate and practical way, appropriate to a small authority with two employees and no dedicated IT department.

The Council:

- Employs a Town Clerk/RFO (who also undertakes all IT administration)
- Employs one Estates employee
- Has councillors who use personal devices

The Council operates a mixed-device model:

- One employee uses council-owned equipment (laptop and mobile phone)
- One employee uses personal equipment
- Councillors use their own phones and/or laptops
- All users have council-issued .gov.uk email addresses

This policy supports the Council's system of internal control and is designed to demonstrate compliance with AGAR Assertion 10 (proper arrangements for information security and digital resilience).

2. Purpose of the Policy

The purpose of this policy is to:

- Protect council information and personal data
- Reduce the risk of data loss, cyber incidents and misuse
- Set clear, realistic expectations for councillors and staff
- Ensure business continuity despite limited staffing and resources
- Demonstrate that information security risks are identified, managed and reviewed

3. Scope

This policy applies to:

- All councillors
- All employees
- Any contractors or volunteers authorised to access council systems

It applies regardless of:

- Whether council or personal equipment is used
- Working location (office, home, or remote)

4. Governance, Roles and Responsibilities

4.1 Town Clerk

As the Council has no IT department, the Town Clerk is responsible for IT oversight, including:

- Day-to-day management of systems and accounts
- Maintaining this policy and reviewing it periodically
- Acting as the first point of contact for IT issues or incidents
- Liaising with external IT or support providers where required

4.2 Users (Councillors and Staff)

All users are responsible for:

- Following this policy
- Taking reasonable care of devices and information
- Reporting any loss, theft, or suspected security incident promptly

5. Equipment and Devices

5.1 Council-Owned Equipment

Council-owned equipment must:

- Be used for council business only
- Be kept secure and not shared with others
- Be protected with passwords or PINs

Any faults, damage or loss must be reported to the Town Clerk without delay.

5.2 Personal Devices

The Council permits the use of personal devices for council business where necessary and proportionate.

Where personal devices are used:

- They must be protected by a strong password, PIN or biometric lock
- Devices must lock automatically after inactivity
- Operating systems and apps must be kept up to date
- Council emails must only be accessed via the council .gov.uk account

Users acknowledge that:

- The Council cannot provide technical support for personal devices
- In exceptional circumstances (e.g. legal or data protection matters), access to council data on a personal device may be required

6. Information Security and Data Protection

6.1 Access Control

- Each user must have their own login credentials
- Passwords must not be shared
- Multi-factor authentication must be used where available
- Computers must be password protected
- Email must be password protected
- Mobile devices must be password protected
- Flash drives must only be used where necessary and must be password protected
- External hard drives must only be used where necessary and must be password protected
- Cloud access is password protected
- Hard copy files are only held where absolutely necessary and must be held securely
- Anti-virus software must be up to date
- No one outside the council must have access to council information

6.2 Storage of Council Data

- Council data should be stored in approved council systems (e.g. council email, cloud storage)
- Council data must not be stored long-term on personal devices where avoidable
- Sensitive documents must be password-protected

6.3 Loss, Theft or Breach

Any actual or suspected:

- Loss of a device
- Unauthorised access
- Data breach

must be reported to the Town Clerk as soon as possible so appropriate action can be taken.

7. Remote and Flexible Working

Remote working is permitted but increases security risk. Users must:

- Ensure screens cannot be overlooked in public places
- Avoid using unsecured public Wi-Fi for council work
- Log out of accounts when not in use
- Keep paper records secure and dispose of them appropriately
- Not leave computers in a public area

Council systems must not be accessed from shared or public computers.

8. Email (to be read alongside Email Guidelines Policy)

- Council email accounts are for council business only
- Users must be alert to phishing emails and suspicious links
- Attachments containing personal or sensitive data should be password-protected

- All councillors, volunteers and staff must adhere to the best practices detailed in the Email Guidelines policy
- All councillors, volunteers and staff must comply with copyright law and must not download or distribute unlawful material using council systems.

9. Internet Use

Usage of council internet access granted for business reasons during working hours is limited to work related activities. The availability and variety of information on the Internet has meant that it can be used to obtain material considered to be offensive. Anyone found to have used the internet to access and/or distribute any kind of offensive material, or non-related employment issues, are liable to disciplinary action which could lead to dismissal.

Under no circumstances must users download files which they suspect contain malware, spyware or may otherwise cause harm to council internet or equipment.

Anyone believed to have been visiting pornographic sites, downloading or circulating pornographic material will be subject to disciplinary action. Offences of this nature may be considered gross misconduct and lead to your dismissal, and if necessary, the police will be informed.

10. Social Media

Social media is a collective term used to describe methods of publishing on the internet. This covers all forms of social media and social networking sites including chat sites.

The use of social media does not replace existing forms of communication.

The policy sits alongside relevant existing polices which need to be taken into consideration. The current Code of Conduct applies to online activity in the same way it does to other written or verbal communication. Individual Town councillors and council staff are responsible for what they post in a council and personal capacity.

In the main, councillors and council staff have the same legal duties online as anyone else but failure to comply with the law may have more serious consequences.

Social media may be used to

- Publish information about the work of Caistor Town Council to a wider audience.
- Distribute agendas, post minutes and dates of meetings
- Advertise dates of meetings, events and activities
- Good news stories linked to website or press pages
- Advertise Job Vacancies
- Re-tweet or share information from partner agencies such as Principal Authorities, Police, Library, Health etc
- Announcing new information
- Post or Share information from other Town related community groups such as hall users, schools, sports clubs, community groups and charities

When using social media (including email) Town councillors and council staff must be mindful of the information they post in both a personal and council capacity and keep the tone of any comments respectful and informative.

Online content should be accurate, objective, balanced and informative. Town councillors and council staff must not:

- hide their identity using false names or pseudonyms
- present personal opinions as those of the council
- present themselves in a way that might cause embarrassment to the council
- post content that is contrary to the democratic decisions of the council
- post controversial or potentially inflammatory remarks
- engage in personal attacks, online fights and hostile communications
- use an individual's name unless given written permission to do so
- publish photographs or videos of minors without parental permission
- post any information that infringes copyright of others
- post any information that may be deemed libel
- post online activity that constitutes bullying or harassment
- bring the council into disrepute, including through content posted in a personal capacity
- post offensive language relating to all protected characteristics including race, sexuality, disability, gender re-assignment, age, marriage & civil partnership, pregnancy and maternity, religion or belief, sex or sexual orientation
- conduct any online activity that violates laws, regulations or that constitutes a criminal offence

Publishing untrue statements about a person which is damaging to their reputation is libel and can result in a court action and fine for damages. This also applies if someone else publishes something libellous on your social media site. A successful libel claim will result in an award of damages against you.

Posting copyright images or text on social media sites is an offence. Breach of copyright will result in an award of damages against you.

Publishing personal data of individuals without permission is a breach of Data Protection legislation is an offence.

Publication of obscene material is a criminal offence and is subject to a custodial sentence.

Councillor's views posted in any capacity in advance of matters to be debated by the council at a council or committee meeting may constitute Pre-disposition, Predetermination or Bias and may require the individual to declare an interest at council meetings.

Anyone with concerns regarding content placed on social media sites that denigrate Town councillors, council staff or residents should report them to the Clerk of the Council.

Misuse of social media content that is contrary to this and other policies could result in action being taken.

The Council will appoint a nominated person as moderator of Town council social media output and be responsible for posting and monitoring content to ensure it complies with the Social Media Policy.

The moderator will have authority to remove any posts made by third parties from council social media pages which are deemed to be of a defamatory or libellous nature.

In summary, councillors and staff must:

- Distinguish clearly between personal views and council business
- Not claim to speak on behalf of the Council unless authorised
- Avoid posting anything that could damage the Council's reputation or breach confidentiality

The Town Clerk is the main point of contact for media enquiries.

11. Monitoring and Proportionate Oversight

The Council reserves the right to:

- Monitor use of council systems where necessary and proportionate
- Access emails or files for business continuity, legal or security reasons

Monitoring will be limited, justified and compliant with data protection legislation.

11. Misuse

Misuse of council systems or data may result in:

- Removal of access
- Disciplinary action (for employees)
- Referral to the appropriate standards or complaints process (for councillors)