ASHINGTON TOWN COUNCIL INFORMATION TECHNOLOGY POLICY

1. Introduction 2

2. Purpose of the IT Policy 3

3. Monitoring of IT Use 3

4. Scope of this policy 3

5. Computer use 4

a) Hardware 4
b) Portable equipment 4
c) Use of own devices 5

6. Health and safety 8

7. Password and Authentication Policy 8

a) Access to Passwords 9
b) Password Storage and Management 9
c) Password Change Requirements 9
d) Password Access Control and Logging 9
e) Responsibility 10

8. Monitoring 10

9. Remote working 11

10. Email 11

11. Emails containing personal information 12

12. Use of the Internet 13

a) Copyright 13
b) Trademarks, links and data protection 14
c) Accuracy of information 14

13. Use of social media 14

14. Misuse 15

ASHINGTON TOWN COUNCIL INFORMATION TECHNOLOGY POLICY

1. Introduction

Ashington Town Council is committed to good governance and the responsible use of public resources. As an employer and as a local authority managing a broad range of services across Ashington, the Council has, over time, developed and adopted a suite of policies designed to ensure it operates lawfully, transparently, and in the best interests of the communities it serves. These have included a Data Protection Policy and Privacy Policy, a Model Publication Scheme, a Press & Media Policy, and a Social Media and Email Policy.

Whilst those policies have provided a sound foundation, a dedicated IT Policy is now required to meet the obligations introduced by the 2025 edition of the Practitioners' Guide, published by the Smaller Authorities' Proper Practices Panel (SAPPP). Paragraph 1.54 of that Guide states that all smaller authorities (excluding parish meetings) must have an IT policy explaining how councillors, clerks, and other staff should conduct council business in a secure and lawful way when using IT equipment and software — whether authority-owned or personal devices. Compliance with this requirement is assessed under Assertion 10 of the Annual Governance Statement (Section 1 of the Annual Governance and Accountability Return), which the Council must complete for the 2025/26 financial year onwards.

Assertion 10 brings together a series of requirements around digital, data, and information governance that were previously captured, less explicitly, under Assertion 3. It requires the Council to demonstrate compliance across four principal areas:

Email and domain governance. The Council must use generic email accounts hosted on a domain owned and controlled by the authority. Personal or free email services (such as Gmail or Outlook.com) must not be used for council business. Ashington Town Council's existing Social Media and Email Policy has addressed aspects of email conduct, but Assertion 10 formalises the requirement for council-owned domain email as a matter of proper practice and data governance.

Website accessibility and transparency. The Council's website must comply with the Web Content Accessibility Guidelines (WCAG) 2.2 AA standard and must publish all documentation required by the Freedom of Information Act 2000 and the Transparency Code for Smaller Authorities. The Council's Model Publication Scheme and existing transparency practices provide a strong starting point, but Assertion 10 requires these to be underpinned by demonstrable technical compliance and an up-to-date published accessibility statement.

Data protection compliance. The Council must demonstrate that it processes personal data lawfully, fairly, and in accordance with the principles of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, recognising its responsibilities as both a Data Controller and, where relevant, a Data Processor. The Council's existing Data Protection Policy and Privacy Policy have given effect to these obligations since 2018; Assertion 10 makes compliance more visible and formally

accountable through the AGAR submission process. This is not a new obligation, but the requirement to assert compliance publicly and annually raises the bar for how compliance is evidenced and maintained.

IT security and acceptable use. The Council must have a documented IT policy setting clear expectations for the secure and lawful use of digital equipment and systems by all who conduct council business — covering both council-owned and personal devices. Whilst the Council's Social Media and Email Policy has addressed some aspects of online conduct, and data protection documentation has touched on information security, a standalone IT Policy is needed to bring together the full range of requirements in one place: password management, device security, remote working, acceptable use, monitoring, and the responsibilities that apply when councillors or staff use personal devices for council purposes.

This IT Policy therefore builds upon and complements the Council's existing policy framework. It does not replace the Data Protection Policy, Privacy Policy, or Social Media and Email Policy, but sits alongside them to address the specific requirements of Assertion 10 and to ensure that the Council can demonstrate, with confidence, that it operates its digital and information systems responsibly, securely, and in accordance with the law. Taken together, these policies reflect Ashington Town Council's commitment to strong governance, public accountability, and the protection of the personal information entrusted to it by the community.

2. Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, staff, and other authorised users use council-provided technology or equipment in the course of their duties. A well-defined policy helps to:

- Set expectations for appropriate use of equipment and systems;
- Raise awareness of risks associated with IT use;
- Safeguard the council's data and digital assets;
- Clarify what constitutes acceptable and unacceptable use;
- Outline the consequences of policy breaches.

3. Monitoring of IT Use

As an IT provider, the council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address

4. Scope of this policy

ASHINGTON TOWN COUNCIL INFORMATION TECHNOLOGY POLICY

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

5. Computer use

a) Hardware

Ashington Town Council computer equipment is provided for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of 'the clerk"). Any personal use of our computers and systems should not interrupt our daily council work in any way. Councillors, staff, and other authorised users are asked to restrict any personal use to official lunch breaks or before or after working hours.

Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

All computer and mobile equipment is assigned to individuals, although shared use may apply to PC's and Laptops. An assets register is maintained.

Equipment should not be dismantled or reassembled without seeking advice.

Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software). Unless previously authorised.

Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the Clerk.

Any faults or necessary repairs must be reported to the Clerk.

b) Portable equipment

Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

All portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018. We will use this wherever possible.

If an item of portable equipment is lost or damaged this should be reported to the Clerk. If the loss or damage is due to an act of negligence, the individual responsible may be required to contribute to the replacement.

To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior written permission of the Clerk. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Clerk.

c) Use of own devices

Personal laptops and other computers or other devices should not be brought into work and used to access council IT systems during working hours, unless this has been authorised by the Clerk. This is to ensure that no viruses enter the system, to prevent

time being wasted during working hours on personal use and to assist in maintaining security, confidentiality, and data protection.

The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's Google Drive or to store data on the council's server(s) or access data in other services. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

However, the same security precautions apply to personal devices as to the council's desktop equipment. The Council recognises that councillors and staff will on occasion use personal mobile phones to make or receive calls in connection with council business, and that this is an accepted part of how the Council operates in practice. Where this occurs, individuals should be mindful that personal numbers may be stored by the recipient and are encouraged to use council-provided contact numbers wherever practicable — particularly for regular or formal communications with contractors, partner organisations, or members of the public. Any emails sent from personal devices must be sent from a council email account and must not identify the individual's personal email address.

Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, we may terminate the worker agreement. This is irrespective of the ownership of the device used. An example would be downloading copyright music illegally or accessing pornographic material.

In cases of legal proceedings against the council, employees or Cllrs, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

ASHINGTON TOWN COUNCIL INFORMATION TECHNOLOGY POLICY

Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a 6-digit pin, strong password, finger print, or facial recognition to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after three failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 5 minutes;
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- for smartphones and tablets, activate the automatic device wipe function (where available). Note that use of the remote wipe function may also involve the removal of the individual's personal data. Councillors, staff, and other authorised users are therefore advised to keep personal data separate from council data where possible;
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

Personal data relating to councillors, staff, associates, residents, and external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

The Council acknowledges that councillors are not routinely provided with council-owned devices and that it is therefore standard and accepted practice for councillors to receive and read council papers, agendas, and related correspondence on personal devices. This does not require prior authorisation. Councillors using personal devices in this way should nonetheless apply the security expectations set out in this policy, including keeping devices updated, using strong passwords or biometric lock screens, and not forwarding council documents to personal or non-council email accounts.

If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

When you open an attachment on a personal device, your phone or tablet may automatically save a copy of that document without you realising it. Once you have finished reading it, please check your downloads folder or the app you used to open it and delete any saved copies. If you are unsure how to do this, the Administration and Communications Officer can help. This matters because if your device is lost, stolen, or picked up by someone else, any council documents saved on it could be read by people who should not have access to them.

Non-confidential agenda papers, minutes, and supporting documents are published on the Council's website and councillors and staff are encouraged to access them there rather than downloading attachments to personal devices. Confidential papers, including those relating to staffing matters or items exempt under Schedule 12A of the Local Government Act 1972, will continue to be distributed by email and should be treated with particular care in accordance with the guidance above.

Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors, staff, and other authorised users are required to allow access, by the Clerk, to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

6. Health and safety

Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the council’s Health and Safety Policy.

Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk.

If any hazards are detected at a workstation, including ‘noises’ from the IT equipment, this should be reported immediately to the Clerk.

7. Password and Authentication Policy

ASHINGTON TOWN COUNCIL INFORMATION TECHNOLOGY POLICY

All user accounts must be protected by strong, secure passwords.

In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

a) Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair, in a sealed envelope, only to be accessed in an emergency.

b) Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a protected system.

c) Password Change Requirements

- Immediately change password if compromise is suspected.

d) Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.

e) Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

8. Monitoring

The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

All computers will be periodically checked and scanned for unauthorised programmes and viruses.

9. Remote working

Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home or at any other venue or premises), as follows:

- if logging into the council's systems or services remotely, using computers that either do not belong to the council or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), council services should not be accessed from that device;
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
- any data printed should be collected and stored securely;
- all electronic files should be password protected and the data saved to the council's system/services when accessible;
- papers, files or computer equipment must not be left unattended at any time;
- any data should be kept safely and should only be disposed of securely;
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed;
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft;

10. Email

Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky.

Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask the Clerk rather than assuming they know the right answer.

All councillors, staff, and other authorised users who need to use email as part of their role will be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

Email messages sent on the council's account should be for council use only. Personal communications are permitted provided they do not encroach upon working time or interrupt council business in any way. Employees and other authorised users are asked to restrict their personal use to official lunch breaks or before or after working hours, and to use their personal email accounts, rather than council addresses.

11. Emails containing personal information

Emails received from residents, councillors, or other parties will sometimes contain personal information such as names, addresses, or photographs. Under the UK GDPR, the Council must only retain personal data where there is a clear and lawful purpose for doing so. Staff and councillors should therefore apply the following approach when receiving emails of this kind.

If the email relates to a matter you are responsible for and need to act upon, retain it in accordance with the Council's document retention schedule.

If the email has been copied to you without a clear reason, or relates to a matter that is not your responsibility, you should not retain it unnecessarily. Delete it once you have read it and do not forward it without the sender's permission.

If you are unsure whether you need to keep an email containing personal information, speak to the Clerk before taking any action.

ASHINGTON TOWN COUNCIL INFORMATION TECHNOLOGY POLICY

To support consistent and lawful handling of unsolicited emails containing personal information, the following standard response should be saved and used where appropriate:

Dear [Name],

Thank you for your email. The information you have shared does not relate to a matter that I am responsible for or involved in. Because your email contains personal information, I will not retain it unnecessarily.

In line with data protection requirements under the UK General Data Protection Regulation (UK GDPR), organisations should only keep personal data where there is a clear purpose for doing so. As the Council is adopting strengthened IT and information governance practices, staff are required to minimise the personal information they hold and only retain information that they need in order to carry out their role.

For that reason, I will delete your email from my inbox and records.

Without your permission I cannot forward the email, so if you remain unsure who to contact, please ring the office. Thank you for your understanding.

Further guidance on data protection, the Council's lawful bases for processing personal information, and retention periods is set out in the Council's Data Protection Policy.

12. Use of the Internet

a) Copyright

Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

It is easy to copy electronically, but this does not make it any less an offence. The council’s policy is to comply with copyright laws, and not to bend the rules in any way.

Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the ‘public domain’ (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk if unsure about anything.

b) Trademarks, links and data protection

The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages to any other external sites without checking first with the Clerk.

Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is available on the Council's website.

c) Accuracy of information

One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

13. Use of social media

The Council's Social Media & Email Policy sets out the standards of conduct, content, and communication that apply to all councillors, staff, and other authorised users when using social media for council purposes or in a personal capacity where the Council's reputation may be affected. This section of the IT Policy addresses the technical and security aspects of social media use and should be read alongside that policy.

Council social media accounts must be protected by strong, unique passwords and two-factor authentication must be enabled on all platforms where it is available. Login credentials for council accounts must never be shared by email or messaging, and access must be reviewed and updated whenever a member of staff with account access leaves the Council.

Social media must not be used to share, forward, or post any personal data, confidential information, or council documents unless this has been explicitly authorised. Councillors and staff should be particularly mindful that photographs, screenshots, and shared documents can contain personal information that is not immediately obvious — for example, metadata, background detail, or visible contact information.

Where council business is conducted through direct or private messaging on social media platforms, those communications may constitute a council record and could be subject to a Freedom of Information or Subject Access Request. Such messages should be treated with the same care as email correspondence and, where relevant, reported to the Clerk so that a record can be maintained.

Personal devices used to access council social media accounts are subject to the same security expectations as council-owned equipment, as set out elsewhere in this policy. If a personal device used to access a council social media account is lost or stolen, this must be reported to the Clerk immediately so that account passwords can be changed and access revoked if necessary.

For all matters relating to conduct, content standards, authorisation to post, use of AI tools, monitoring, and disciplinary consequences, refer to the Council's Social Media & Email Policy.

Note that the council may, from time to time, monitor external postings on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the council. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air council concerns or complaints: these should be raised with the council or formally through the grievance procedure.

It is important to note that officer, councillor and stakeholder contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including external stakeholders contact details from any personal device/equipment.

14. Misuse

Use of IT systems and equipment that is not in line with the council’s standards of conduct will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.