



# **HARWICH TOWN COUNCIL**

## **IT POLICY**

THIS DOCUMENT OUTLINES THE POLICY ADOPTED BY  
HARWICH TOWN COUNCIL

Date of policy: February 2026  
Approving committee: Full Council  
Date of committee meeting: 24.02.26  
Policy version reference: V1  
Supersedes: N/A  
Policy effective from: 24.02.26  
Date for next review: February 2029

## **Scope & Purpose of the IT Policy**

The purpose of this 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. This 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.

Harwich Town Council will also determine and clearly state whether limited personal use of IT equipment is permitted (for example, checking personal email or online shopping during lunch breaks).

This policy applies to all councillors, staff, and other authorised users, regardless of working location or pattern, including those who are home-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.

This policy relates to all information technology facilities and services provided by the council. All the council's IT facilities and information resources remain the property of Harwich Town Council.

## **Monitoring of IT Use**

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.

## **Computer use**

### **1.1 Hardware**

**1.1.1** Council-owned computer equipment is provided for council purposes, however reasonable personal use is permitted so long as such use does not incur specific expenditure on the council, occur during working hours or impact on job performance, break the law or bring the council into disrepute. Personal use is restricted to official breaks or before or after working hours.

**1.1.2** 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.

**1.1.3** All computer and other electronic equipment supplied should be treated with good care at all times.

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

**1.1.5** All computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

**1.1.6** Equipment should not be dismantled or reassembled without seeking advice.

**1.1.7** Councillors, staff, and other authorised are not to purchase any IT equipment on behalf of the council without express authorisation. All purchases should be authorised by the Clerk and expended from the IT budget.

**1.1.8** Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on council computers without express authorisation.

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

## **Equipment**

### **2.1 Portable equipment**

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

**2.1.2** Council back-up procedures specific to portable equipment should be followed at all times.

**2.1.3** All portable computer equipment 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 and should not be left unattended when away from council premises or left in parked vehicles.

**2.1.4** All portable computer equipment that holds council data, including emails and files, must be protected with a password/pin. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security settings must not be disabled or removed.

**2.1.5** Where possible Multi-Factor Authentication should be applied to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

**2.1.6** 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 liable to costs or disciplinary action.

**2.1.7** To protect confidential information, unless it is a requirement of the role, it is forbidden for photographs or videos to be taken on council premises, without the prior consent from the Clerk. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

**2.1.8** 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).

**2.1.9** 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.

## **2.2 Use of personal devices**

**2.2.2** Councillors, staff, or other authorised users may wish to use their own device(s) to access servers, private clouds or networks for normal council purposes, including, but not limited to, reading emails, accessing documents or storing data. Any use of personal devices is at the discretion of the council, and consent will normally be permitted. Any 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.

**2.2.3** The same security precautions apply to personal devices as to the council's equipment. For continuity purposes, unless software is installed to prevent personal data being disclosed (e.g Webex), calls should be made from the council landline to ensure that only these numbers are used and/or stored by the recipient. Any emails sent from personal devices should be sent from a council email account and should not identify the individual's personal email address.

**2.2.4** Councillors, staff, and other authorised users 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 council's IT infrastructure, 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.

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

**2.2.6** 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, by using different accounts for council and personal use. If the device supports multiple profiles, the work/council profile must always be used for work or council-related purposes.

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

- use a strong password or pin to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after a set number of failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity;
- 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;
- install appropriate anti-virus;
- 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.

**2.2.8** Personal data relating to councillors, staff, associates, residents, external stakeholders and other authorised users 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.

**2.2.9** Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people

**2.2.10** 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.

**2.2.11** Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use to avoid data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

**2.2.12** Any work done on user's own equipment should be stored securely, password protected and should always be backed up in accordance with the council's standard backup procedures.

**2.2.13** If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (<https://>). Unsecured wireless networks should not be used.

**2.2.14** Prior to the disposal of any device that has work data stored on it, and in the event of leaving the council, councillors, staff, and other authorised users are required to allow the council or its designated IT services provider access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

**2.2.15** Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work when using these to access council servers/equipment. Risks to the user's personal device(s) include data loss, bugs and viruses, software or hardware failures and programming errors. The council will use reasonable endeavours to assist, users are personally liable for adequately protecting their own device(s) and for any costs incurred as a result of the above.

## **Health and safety**

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

**3.1.2** 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.

**3.1.3** 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.

## **Password and Authentication Policy**

**4.1.1** All user accounts must be protected by strong, secure passwords. The council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks.

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 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 website provider.

### **4.1.2 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 must be granted to authorised personnel from the IT provider.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the chairman of the council, in a sealed envelope, only to be accessed in an emergency.

### **4.1.3 Password Storage and Management**

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using an encrypted password manager.

### **4.1.4 Password Change Requirements**

- Passwords should be changed frequently and immediately if compromise is suspected.

### **4.1.5 Password Access Control and Log In.**

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

#### **4.1.6 Responsibility**

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

The IT provider is responsible for:

- Managing system/service credentials.

#### **Monitoring**

**5.1.1** 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 may be monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

**5.1.5** 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.

**5.1.6** Monitoring of an employee's email and/or internet use will be conducted in accordance with this policy. Monitoring is in the council's legitimate interests and will always be necessary and proportionate.

**5.1.7** The information obtained through monitoring may be shared internally, including with relevant councillors and IT services provider. 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.

**5.1.8** 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.

**5.1.9** 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.

**5.1.10** 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.

**5.1.11** 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.

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

## **Remote working**

**6.1.1** 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 premises or any other different venue), 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 device 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 unless arrangements have been made with a responsible person to be kept in a locked room or cabinet.
- 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. If staying away overnight, all devices should be taken into the accommodation, care being taken that they 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;
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.
- Ideally, remote access software should be used to avoid council data being stored directly on the device.

**6.1.2** Use of a council issued 'dongle' that enables internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should be used for essential council purposes only, especially if abroad.

**6.1.3** Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

## **Email**

**7.1.1** Council email facilities are intended to promote effective and speedy communication on work-related matters. 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.

**7.1.2** Emails should not be used as a substitute for face to face or telephone conversations.

**7.1.3** All councillors, staff, and other authorised users who use email as part of their role will be provided with a council owned email address and account. Personal email addresses are not to be

used for council business and the council will only accept communications from councillors and staff from their council-owned email address. 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.

**7.1.4** Emails sent using the council's account are for council use only. Personal use is not permitted.

## **Use of the Internet**

### **8.1 Copyright**

**8.1.1** Any use of copyright materials permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws apply to documents and 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.

**8.1.2** The council's policy is to comply with copyright laws.

**8.1.3** 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).

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

### **8.2 Trademarks, links and data protection**

**8.2.1** 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 Council.

**8.2.2** 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 from the Clerk.

### **8.3 Accuracy of information**

**8.3.1** The internet provides access to large amounts of information, which may be less accurate than it appears.

## **Use of social media**

**9.1.1** Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV

and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

**9.1.2** Personal use of social networking/media and chat sites are not permitted during working hours and should be restricted to breaks during working hours, or after hours with permission.

**9.1.3** Where it is relevant for councillors, staff and other authorised users to use social networking sites as part of their role, this is acceptable.

Inappropriate comments and postings can adversely affect the reputation of the council. If comments or photographs could reasonably be interpreted as being associated with the council, or if remarks about external stakeholders could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence. Councillors, staff, and other authorised users should take care when expressing any views on personal weblogs, even if the council is not named.

**9.1.4** To protect both the council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:

- Contacts from any of the council's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions the council, its current work, councillors, employees, other users associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of the council. Care should be taken with any views expressed on social media sites and any views should clearly be stated to be the writer's own (e.g. via a disclaimer statement such as: *"The comments and other content on this site are my own and do not represent the positions or opinions of my employer/ the council."*) Writers must not claim or give the impression that they are speaking on behalf of the council.
- Any employee who is developing a site or writing a blog that mentions the council, its plans, councillors, staff, or other authorised users, and partners, must seek permission from the clerk before going 'live'.
- The council expects users to be respectful about the council and its current or potential councillors, staff, volunteers and anyone else associated with the council, not to engage in any name calling or behaviour that could reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.
- Photos or videos that include employees or other workers wearing uniforms or clothing displaying the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission.
- Comments posted by councillors, staff, and other authorised users on any sites should be accurate and professional and should not compromise the council in any way.
- Inappropriate conversations with external stakeholders should not take place on any social networking sites, including forums.

- Any writing about or displaying photos or videos of internal activities that involves current councillors, staff, and other persons associated with the council, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission should be gained prior to uploading any such material. Details of any kind relating to any events, conversations, materials or documents that are meant to be private, confidential or internal to the council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users; anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.
- Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as such. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.
- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about the council or it's councillors, staff, volunteers or anyone else associated with the council, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council, should be referred to the Clerk.
- Councillors, staff, and other authorised users who use sites such as LinkedIn and must ensure that the information on their profile is accurate and up to date and must update their profile on leaving the council.
- Councillors, staff, and other authorised users who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council or its councillors, staff, anyone else associated with the council, on LinkedIn, Facebook, X.com or any other social media/networking sites.
- Any professional contacts and/ or confidential information created or obtained in your capacity as a councillor, staff, or other authorised user will be considered council property and may be subject to disclosure upon request.

**9.1.5** 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.

**9.1.6** External stakeholders' contact details and information remain the property of the council and 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.

### **Misuse**

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