Skipton Town Council

Policy Name:	**Information Systems Policy**
Date of Last Review:	**14 May 2026**
Version Number:	**v1**
Responsible Officer:	**Chief Officer**
File Location:	**Shared Drive**
Next Review Due:	**May 2027**
Added to Policy Register:	**YES/NO**

1.0 Introduction and Context

The purpose of this document to set out the rules for all staff & Councillors on their usage of corporate IT systems and tools and handling information in all formats. The Policy is intended to allow Employees and Councillors to make the best use of resources, whilst at the same time Safeguarding the Council.

2.0 Scope

This policy covers all STC staff & Councillors.

3.0 Aims & Objectives

The rules have been designed so that they enable Skipton Town Council (STC) to manage information security risks to an acceptable level, whilst also recognising the flexible ways in which staff need to work: in the office, at home, on the move and on occasions using personally-owned devices. The rules also balance the need for compliance
– such as with Data Protection law - and other business requirements of STC with the privacy and practical needs of staff as individuals

4.0 Terminology & definitions

‘Staff’ or ‘member of staff’ for the purposes of this policy means anyone directly employed by STC or anyone engaged in work for STC in any capacity (i.e. regardless of their tenure, or working via an agency, casual staff etc.), who is given access
to STC computing resources and/or STC information to carry out work for or on behalf of STC as a legal entity and a data controller as defined by GDPR/Data Protection Act (2018).

Although Councillors are not STC ‘employees’ or ‘staff’ they are also within scope of this policy where they are given access to STC information systems in order to carry out their

Council business.
‘Information Systems’ primarily relates to staff use of IT such as network, infrastructure, computing devices and specific digital tools, but also includes the acceptable use of information in any other formats such as paper files.

‘STC-owned information’
Any information held by STC to perform its business – which includes HR-type personal data on staff - remains STC-owned information regardless of whether it is accessed by a STC-owned device or a personally-owned device (i.e. a device such as a laptop or smart phone which is owned and controlled by staff) and regardless of how it is stored.
‘Personally-owned information’ is that information which staff have obtained or created which is not relevant or necessary to STC business and relates to their life outside STC and should not be stored on STC systems.

‘Personally-owned device’ for the purposes of this policy is defined as items of equipment such as phones, laptops and tablets which are selected, paid for, maintained and controlled by individuals primarily to help them in their personal non-work lives. Increasingly, these devices can also be used to access some STC services (e.g. email and SharePoint). This is often known as ‘Bring Your Own Device’ (or BYOD). This policy sets out the ground rules for such access.

5.0 Risks & Cyber Security

This policy has been designed so that STC can reduce the cyber threats which seek to exploit staff behaviours and unacceptable usage of information systems (e.g. an attacker obtaining a password used via social media which is the same one for access to SCC or accessing SCC network using a laptop which has not been secured).

6.0 Responsibilities

This policy sets out the individual responsibilities for ALL staff & Councillors. In the case of any malicious activity, all staff & Councillors need to know that over and above STC disciplinary procedures relating to not conforming to this staff information systems usage policy, action could be taken against them as individuals under GDPR/Data Protection Act (2018) and Computer Misuse Act (1990) or other law.

Managers are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy.

The Chief Officer is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them so as to implement this policy.

7.0 Users

Any breach of this policy by staff could warrant further action and investigation under the Council’s Disciplinary Procedures. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

Councillors found to be in breach of this policy may be deemed to have breached the

Members' Code of Conduct and may lead to a referral to the Craven District Council's Monitoring Officer.

8.0 Joining, moving within and leaving STC

8.1 Issuing of IT Equipment

It is the responsibility of the Chief Officer to ensure that the right equipment (together with initial access rights to services) has been ordered prior to the new member of staff joining and that new staff know how to use their equipment within the context of STC. This may include one or a combination of desktop, laptop, smart phone etc

It is assumed that new staff have satisfactory proficiency in IT prior to joining STC (i.e. use of devices and passwords, Internet-browsing, use of standard word processing and spread-sheet packages etc.). STC line managers are responsible for ensuring specific tools (e.g.Realtis) and specific security controls are explained prior to such tools being used. It is the responsibility of all staff to safeguard their official laptop/smart phone devices by ensuring they are shut down, put in a bag and taken home at the end of each day or locked away in the office. Any loss of such equipment must be reported to the Chief Officer.

STC equipment issued to staff has been set up to minimise cyber and other risks. Staff must not attempt to tamper with this official equipment by seeking to change hardware or software settings or bypass any security features. It is not permissible for staff to seek assistance from any person or company (other than STC and its approved contractors) to analyse or repair or change STC devices in any way.

It is not permissible for anyone other than IT to disconnect and move non-portable equipment such as desktop computers, scanners, servers etc. to other locations.

It is not permissible for any staff to attempt to introduce and set up their own IT or similar equipment on STC premises. This includes, but is not limited to, surveillance cameras, wired or wireless routers, printers, scanners and non-STC managed laptops or tablets etc.

8.2 Passwords

A password will be issued to staff that relates to their logon to the STC network and core systems. This should be memorised and should not be shared with anyone. Passwords must not be kept with or attached to the device.

Additionally, depending on job role, there may be one or more passwords or other credentials required to use information systems/tools such as the financial software system.

It is the responsibility of staff to safe-guard such passwords and not to share them.

The IT Services Provider has the authority to force any member of staff to change a password at any time if, in its judgement, there is a security issue (e.g. a password has been compromised).

All staff have a responsibility to report any security issues – such as possibility of password being compromised – immediately to the Chief Officer and the IT Services Provider.

8.2.1 Access permissions

All staff should be able to access and share the information they need for their role(s) in STC.

Staff will have their own specific permissions based on roles and other criteria (e.g. for contractors/temporary staff), and line managers have a responsibility to explain them to their staff.

Note: not all access permissions can be upheld by technical permissions (i.e. just because the IT system or service allows you to view data does not mean that you have permission to access it).

All staff need to be able to demonstrate that any access to data in STC systems is:

- legitimate (i.e. you have a relationship with the customer/client)
- time-bound (your current role and current case-work means it is necessary, and
- proportionate (i.e. you can justify the amount and range of data if challenged in the event of a privacy investigation).

Access and actions on STC systems - which all have a form of audit trail - should always be traced to individuals, and staff should not share credentials/passwords or allow others to view or change data using their account.

8.3 Changing roles and extended absence

When a member of staff changes roles within STC, it is the responsibility of line managers to ensure that the access to job-specific systems and information are updated accordingly (e.g. IT access permissions rescinded).

Where a person has changed roles and there is no business need to access information relating to the previous role, the member of staff should not attempt to access such information. In the event of an investigation, the onus will be on the staff member to justify the business need for such access.

When a member of staff is due to be absent (or has been absent) from STC for any reason including maternity, sickness, career break, disciplinary, outward secondment etc.) for more than 30 days then IT must be notified, and all STC equipment returned and access to all information systems ended.

Note: the end of access to STC network and information systems does not mean that communications with such staff on temporary absences should be ended, as ‘staying in touch’ is important. Instead, other means should be found to communicate such as telephone calls, emailing to personal accounts.

8.4 Leaving STC

It is the responsibility of Chief Officer/Deputy Clerk to inform IT when a member of staff is due to leave STC no less than one week prior to the member of staff’s leaving date.

It is the responsibility of the Chief Officer/Deputy Clerk to arrange for the handing in of all IT equipment and photo identification pass prior to leaving the building on or prior to the last

day of work. The member of staff will be asked to sign a Leavers' Declaration form confirming this.

It is the responsibility of all staff to hand in to line managers any IT equipment such as phones, laptops, any removable media or paper files as well as identification pass prior to leaving and to ensure that corporate information is filed in the correct places. Note: even after leaving STC employment, individuals – including councillors - can be prosecuted under Data Protection and other laws for misusing personal and corporate data relating to a previous employer.

The content in email accounts and in employee-created stores (e.g. OneDrive) will be deleted within 3 months after leaving STC unless there is a business need for it to be retained for a longer period.

9.0 Office Security

9.1 Screen Lock devices when unattended

All portable devices such as laptops must have their screen-locked when left unattended for any length of time. When finishing work, such devices must be shut-down, put in a bag and brought home OR locked away in a lockable cupboard within the office.

9.2 Clear desk policy

STC operates a clear-desk policy. This means while working at a desk/office environment paper files should be kept to an absolute minimum (especially anything which contains personal data) and such papers should be locked away at the end of the working day (i.e. leaving a clear desk) and not left near printers or other work surfaces.

9.3 Wastepaper

Waste paper with information on must be disposed of in designated secure confidential waste bag or shredded.

Waste paper with no personal or sensitive information and in regular recycling paper bins should be recycled.

9.4 Working on the move

It is permissible for staff to access and view STC information in any format (paper or digital) while on the move providing that:

- No personal or sensitive level information can be viewed by non-intended persons (e.g. adjacent seats, passers-by etc.).
- The device, such as a laptop, must be shut-down and placed in a bag and safeguarded when not in use, even for short period.
- The loss of a device must be reported immediately using the STC security incident reporting process.

9.5 Working from Home

It is permissible for staff to access and use STC information including personal and sensitive information in any format (paper or digital) while working at home providing that:

- “Home” is defined as a property such as a flat/house which is lockable and has at least one room which can provide a similar level of privacy to that in a designated STC office space.
- Only a minimal amount of STC paper files or printed outputs are kept at home (i.e. for next day or week of visits/meetings etc.) and should be secured when not in use.
- STC devices can be connected to home Internet wired or wirelessly but must use the STC Direct Access (VPN - Virtual Private Network).
- The device, such as laptops, should be shut-down when leaving your home even for short periods.
- Due care needs to be taken when other residents of the household are present and in shared areas of the home so that non-intended persons cannot view STC information etc.
- Waste paper with STC information on should be machine shredded at home or brought into STC to dispose of in designated secure bins.
- The loss of a device or information must be reported immediately using the STC security incident reporting process.

9.6 Use of personally-owned devices to connect to STC services

It is permissible for staff to access certain STC Internet-based tools (such as SharePoint/email) using their personally owned devices providing that:

- The member of staff is content that his/her personally owned device can be used to access STC services for the convenience that this brings (i.e. rather than being issued with a separate STC owned device).
- The personally owned device to be used meets the minimum technical specification required for the STC services.
- The member of staff understands that although ‘personal life’ applications and data are segregated from STC services as far as possible, there are certain instances where STC will require the user to follow specific instructions and/or downloading security software.
- Such access needs to follow the agreed login process. Where services are accessed in this way, no information should be downloaded/saved onto the personally owned device.
- Any security incident or concern should be reported immediately via the information security reporting process.

10.0 Use of Email

Staff will be provided with an individual STC email account.

- The individual STC email account must only be used by the named member of staff and access must not be shared with anyone else.
- The STC email address/account must not be used to send or receive messages relating to non-STC business.
- Personal non-STC related email accounts must not be used for STC business (other than the business continuity circumstances in section below).
- The STC email address must not be used to register yourself for services that do not relate to STC business (i.e. not linked to personal social media or leisure websites)

- STC email accounts can be used to send all types of information in the body of the email and/or attachments, but if it is deemed to be OFFICIAL-SENSITIVE then he OFFICIAL-SENSITIVE button must be pressed prior to sending the message.
- All staff have a responsibility to avoid opening messages which appear suspicious and to delete them (rather than forward them) promptly.
- STC email should not be used to send any content which is illegal, abusive, threatening, which constitutes spam or chain-mails or would bring the council into disrepute. If a member of staff receives such email, then it should be deleted and not forwarded on to anyone.
- Health and safety of staff: If any such message is targeted at individual members of staff and could have health or safety impacts (e.g. a threat to a member of staff) then the Chief Officer must be informed.
- All staff have a responsibility to report an information security incident where they feel a STC email account has been compromised in some way or if they have inadvertently downloaded something malicious via email.
- Email should be used as means to communicate and must not be used as a record repository (see records management below).

11.0 Telecommuncations

See Mobile Phone Policy

It is permissible for staff in STC to use the following to communicate verbally with others using:

- Fixed telephones in STC offices.
- STC mobile phones
- The use of personally owned non-work fixed and mobile phones are permissible for STC business provided they are only for verbal conversations by mutual agreement of STC staff and line managers.
- Staff should not attempt to move/export any data contained on STC mobile phones such as contact lists onto any other device
- Text messages that relate to STC business should not be sent from/to personally owned mobile

12.0 Use of the Internet

12.1 Browsing Sites

All staff may access the public Internet using STC devices either in the workplace, in the community, on the move or at home.

All staff may use STC computing resources (devices and network) in order to browse the Internet for leisure purposes during breaks at the discretion of line managers provided it does not interfere with work or disrupt other staff (i.e. having audio on). Passwords used to access such non-work sites (e.g. banks, personal email accounts) must be different from those used for STC computing resources and services.

Staff must be aware that the following content is considered inappropriate and should not normally be created, accessed, or stored on any IT facilities or equipment:

- sexually explicit content

- material that gratuitously displays images of violence, injury or death
- material that is likely to lead to the harassment of others
- material that promotes intolerance and discrimination on grounds of age, disability, gender, gender reassignment, marriage and civil partnerships, pregnancy and maternity, race, religion or belief, sexual orientation
- material relating to criminal activity, for example buying and selling illegal drugs
- material relating to any other unlawful activity e.g. breach of copyright
- material that may generate security risks and encourage computer misuse (except where it is strictly and necessarily required for your work, for example audit activity or other investigation

You must not use your Internet enabled user account to:
Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video, image or other in breach of copyright materials

- Subscribe to, enter or use online gambling or betting sites.
- Subscribe to or use “money making” sites such as “paid to click”, “paid for easy tasks” or “paid to create content” sites.
- Access the Internet at STC in order to run a private business.

The above list gives examples of “unsuitable” usage but is neither exclusive nor exhaustive. Such material would include data, images, audio files or video files the transmission of which is illegal under UK law, and, material that is against the rules, essence and spirit of this and other Council policies.

Staff usage of social media in their personal lives (i.e. not the social media administered for STC business) is governed by STC Social Media Policy.

12.2 Downloading Software and applications

It is not permissible for staff to attempt to manually download any software from the public Internet onto any STC device. If new applications or updates are required, then this must be ordered via the IT portal.

Where a member of staff has inadvertently downloaded software/application or enabled something to happen to file types by clicking on something then this should be reported as an information security incident.

It is not permissible for staff to attempt to change any standard settings on devices or attempt to disable any security features (e.g. anti-virus).

All staff must follow STC IT instructions, whether via automated message or other route, to download security updates/patches/versions which are there to safe-guard the entire STC network.

Staff must not make online purchases or enter into any contracts on behalf of STC without the authority of approved procurement procedure.

Social engineering: All staff should take reasonable precautions against following instructions from non-STC staff by phone, email or other channel (i.e. social engineering attacks)

13.0 Storing staff personal information at STC

STC information systems are designed so that only its corporate information – including personal data on customers and staff – are held on them. They must not be used for holding information that relate to what staff do outside of work (e.g. do not file information on your family, friends, social life, personal finances, personal photographs, music files, information on other jobs, hobbies etc.).

The exception is that personal information which is generated during the course of working for STC which employees co-own or generate themselves but is still related to their employment. This information can be legitimately filed in record repositories where the employee has a higher degree of control over and access is limited to individual employees.

This includes (list not exhaustive):

- Copies of annual appraisal and development plans
- Correspondence about personnel matters in STC (e.g. maternity, health, terms and conditions).
- Correspondence generated where Trade Unions membership relates to employment at STC.
- Documents relating to professional activities which overlap with STC (e.g. CVs, registration, accreditation, professional exams, conferences etc.).

Those with line management responsibilities should keep information about the staff they manage in their 'personal' files to an absolute minimum and be mindful that such information may be disclosable in the event of Subject Access Request (SAR) or other legal request. Such information should be filed in:

- Named 'OneDrive' which is designed to hold such information which the employee would consider 'personal' in a work context.
- Designated personal drives for digital files.
- Paper copies filed at home

Note: While held on STC systems, such information can still be made accessible for authorised purposes (e.g. when staff member is absent/business continuity or because of an investigation). When leaving STC, employee-created personal information and individual on STC systems will be deleted within 3 months after leaving the organisation.

14.0 Filing corporate information & records

All staff must file information that they create or receive during their day-to-day work in the appropriate corporate record repositories. One or a combination of the following must be used:

- Team shared drives with a structured folder structure
- Team SharePoint site with structured document libraries
- Team case management system (i.e. to hold information on customers/clients/buildings etc).
- Specific local information systems designed to hold structured information

Staff must not use email as a records management system and should file what is needed to be retained in the above repositories and keep the amount of data inboxes to an absolute minimum.

Use of non-personal accounts
Staff must not file STC information onto personal non-work (e.g. such as emailing to personal email accounts or uploading content onto social media or file-sharing tools).

Any temporary papers printed or hand-written notes for convenience must be securely destroyed if they contain personal or sensitive information at the earliest opportunity (e.g. once formal minutes have been filed).

Paper files
Legacy paper files must be locked away when not in use within STC buildings and should not be left on desks or other work surfaces at the end of the working day.
Payment card and financial details

15.0 External information sharing
All staff need to share information - including personal data – with STC colleagues and external partners where it is lawful and there is a clear business need.

All staff have a duty to query if they are unclear on whether they should be sharing data outside STC.

- Where removable media (such as memory sticks) are to be sent from STC, the data must be on STC encrypted removable media.
- Email should be avoided as far as possible as a means of sharing high volumes of personal data
- Where data is to be shared using an online file-sharing tool, then it must be one which has been approved by STC.

In all cases, regardless of the information sharing tools used, staff need to be clear on:
- who transferred the data (identity of the person in STC)
- when it was transferred
- the destination and evidence that it was received and
- to report an information security incident without undue delay if you suspect that data has been lost, misdirected or compromised.

16.0 Business continuity

Where a member of staff is not available for any reason (e.g. sickness) STC must be able to access all the information that the person would normally access while at work on STC systems – including individual STC email account, STC OneDrive, STC shared drives, STC SharePoint and paper files – for business reasons.

In the event of a business continuity issue and/or invoking of business continuity plan the following are permissible:
- Staff can be contacted using their personally owned email accounts and telephones. It is the responsibility of all staff and The Chief Officer that such out of hours contact lists are kept up to date.
- Specified paper files and STC encrypted media can be brought to other working environments including home in the event of an IT outage.

17.0 Security issues due to staff misuse of systems

All staff are responsible for reporting any incident that they become aware of which impacts on the confidentiality, integrity or availability of information – by reporting to the Chief Officer without undue delay.
Depending on the actual or potential impact of any non-compliance with the staff usage policy, the following will be decided by the Chief Officer in consultation with line managers at any time:

- Suspension of access to some or all STC systems and services.
- Suspension of access to STC Offices.
- Recall of equipment issued to staff to enable forensic analysis.
- Recall of any information in any format such as paper files which may be held by staff.

The above action will be taken in the interests of protecting STC systems or preventing further impact regardless of the circumstances (malicious and non-malicious activity on STC systems).
Where any information security incident is due wholly or partially because staff did not adhere to this usage policy on information systems then the following will apply:

- The Chief Officer will carry out an investigation.
- In the case of potential breaches of personal data, the Chief Officer will seek further advise and liaise with Information Commissioner if necessary.

The IT Service Provider may provide technical (e.g. audit trails) and other data.

- Staff involved in the incident will have an opportunity to explain the circumstances, including why part of the policy was not adhered to.

In the event of potential misuse involving Councillors, the Chief Officer may seek the advise of the monitoring officer.
The Chief Officer will decide with the Management & Staffing Committee whether any disciplinary action is to be taken (in the case of gross misconduct this could lead to dismissal). The IT Provider will provide any necessary technical data to support this, as well as evidence of staff cooperation during its investigation (e.g. handing in equipment and providing details of the incident promptly, not attempting to access systems when asked etc.).
In the case of any malicious activity, all staff need to know that over and above STC disciplinary procedures relating to not conforming to the staff information systems usage policy, action could be taken against them as individuals under GDPR/Data Protection Act (2018) and Computer Misuse Act (1990) or other law.

.

18.0 Related Documents (links to procedures etc)

Code of Conduct
Records Management Policy
Freedom of Information
Security Incident
Social Media Policy

This Policy will be reviewed in two years.