South Derbyshire District Council

PROTOCOL FOR THE USE OF INFORMATION TECHNOLOGY BY MEMBERS OF SOUTH DERBYSHIRE DISTRICT COUNCIL

Version: 2.2

Date: September 2023

Contents

Version Control

Version	Description of version	Effective Date
1.5	Updated to reflect new ICT equipment, member requirements and best practice	April 2018
2.1	Updated to reflect current working practices and guidance	May 2023
2.2	Updated to reflect feedback from cross-party working group	September 2013

Approvals

Approved by	Date

Associated Documentation

Description of Documentation
Elected Member Data Protection Handbook

1.0 Introduction

The SDDC Member ICT Protocol is a document to govern Member use of Information Technology and is not intended to restrict you in carrying out your normal Council activities.

This policy relates to the use of ICT equipment, software and communication network when undertaking official Council duties only.

South Derbyshire District Council provides Members with ICT equipment to reduce costs and improve productivity and digital adoption should be the primary channel of business, as it is with Officers.

The ICT Protocol, which follows, exists for a number of reasons, the most important of which are:-

- To protect the Authority and its Members from prosecution. This can involve Data Protection, software usage, security and virus issues.
- To protect the assets owned by the Authority. These assets include not only software and hardware but also data.
- To standardise the working environment. This will allow every computer to operate the same, wherever you are located.
- To streamline ICT equipment procedures, giving users a faster response to faults.
- To enable Members to carry out their duties safely and more effectively.

In order for access to be granted to the Councils ICT infrastructure a Member must understand and accept this protocol.

Any breach of the Protocol may amount to a breach of the Members' Code of Conduct. In addition, any breach could lead to the equipment being recovered by the Council.

If you require clarification of any issue about the use of ICT, please contact ICT Services on 01283 387500, who will be more than happy to assist.

The Protocol will be monitored and reviewed periodically to consider any appropriate amendments necessary.

All other South Derbyshire District Council District Council codes, guidelines and policies apply in addition to the ICT Protocol

2.0 The role of the Member

1) They will act as a member of the Council undertaking official council business, for example, as member of a committee or sub-committee. As defined in the Code of Conduct a "Councillor" means a member or co-opted member of a local authority or a directly elected mayor. A "co-opted member" is defined in the Localism Act 2011 Section 27(4) as "a person who is not a member of the authority but who
   (a) is a member of any committee or sub-committee of the authority, or;
   (b) is a member of, and represents the authority on, any joint committee or joint sub committee of the authority;

2) They will represent the residents of their ward, for example, when undertaking casework.

3) They will represent a political party, particularly at election time.

Members will process personal data for different purposes depending on which of the above roles they are undertaking. This policy only applies when the elected member acting in the capacity outlined in point one above.

Who is accountable for the personal data, and therefore what devices and communication channels to use, when undertaking these roles?

Official Council duties
When a Member collects, uses and stores personal data when undertaking official Council duties such as attending a Committee, the Council is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Council will do this by providing Members with training, awareness, policies, procedures and guidance so that they know how to handle personal data properly and lawfully.

Undertaking Casework
When a Member collects, uses and stores personal data when undertaking casework, the Member is the Data Controller. The Member is accountable for the data they process as they will determine the means and purpose of processing and must ensure that it is used in the right way. If the Member chooses to use ICT equipment provided by SDDC for their casework they remain the data controller for the lifecycle of the data, however the Council will also be a data controller for data stored on our network and as such will secure its network to prevent data loss. If data breach has occurred from a data loss relating to SDDC networks the Council will report the incident to the ICO

It is assumed by the Council that Elected Members undertaking casework are responsible for knowing and abiding by the data protection principles.

Representing a Political Party
When representing a political party, for example when campaigning at election time, the political party is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Political Party may do this by providing its Members with appropriate training, awareness, policies, procedures and guidance.

Segregation of Duties & Personal Data

Data protection legislation requires that you have a very clear specified purpose for collecting and using personal data.

Once collected for a specific purpose, personal data cannot generally be used for any other purpose unless:

- the new purpose is compatible with the original, (or)
- you get the consent of the individual to use their data for another purpose,(or)
- you are required to use the information in another way by law (e.g. reporting a safeguarding concern).

For Members, the purpose for processing the personal data is linked directly to the role they are undertaking. For example, when representing a constituent, any personal data collected and used is for the specific purpose of dealing with the enquiry or complaint, and must not be used for any other purpose, e.g. political campaigning.

It is therefore important that Members segregate any personal data held for different purposes and roles.

As a Member of the Council

- Councillors may have access to, and process, personal information in the same way as employees e.g. Committee Reports. In this case it is the Council rather than the Councillor that is the Data Controller.
- Council is responsible for ensuring compliance.
- Data Breaches Must be reported to the Councils DPO within 72 Hours.

As a representative of the residents of their ward (Casework)

- When Councillors represent residents of their ward, they are processing personal information in their own right. E.g. using personal information to timetable a surgery appointment or take forward complaints made by local residents.
- It is the Councillor rather than the Council that is the Data Controller.
- The Councillor is responsible for ensuring compliance and reporting any data breaches to the ICO unless the data breach has occurred from a data loss relating to SDDC networks in which case the Council will report the incident to the ICO

As a representative of a political party

- When acting on behalf of a political party, for instance as an office holder, Councillors are entitled to rely upon the registration made by the party to determine how and why personal information is used. It is the Party rather than the Councillor that is the Data Controller.
- The Party is responsible for ensuring compliance. Data breaches should be reported to the Parties DPO.
- If a prospective Councillor is not part of a political party but campaigning to be an independent councillor for a particular ward, the candidate is the Data Controller.

2.0 Access to Authority ICT Systems

This policy relates to the use of ICT equipment, software and communication network when undertaking official Council duties.

In order to gain access to the SDDC systems, such as outlook, OneDrive, SharePoint and exempt information in CMIS it is necessary to have a valid username and password. Your username and password, also known as credentials, will be provided by a representative of ICT.

The password generated and assigned to a user account will follow strict protocol on its composition as documented later in this protocol and recommended by the National Cyber Security Centre.

Access to the Council's network away from Council buildings can only be gained through the use of Virtual Private Network (VPN). In order to access the VPN, users must authenticate through Multi Factor Authentication (MFA). The process of MFA involves a secondary device which a code or prompt can be sent to validate identity. This process is called Identity Management.

Members can choose to have a corporate smartphone to conduct this process or can use their personal device if preferred. Members are encouraged to request a corporate smartphone as this gives secure access to Council services, such as emails, documents and the intranet from any location.

No official council business is conducted through Identity Management and it is recognised that use of a personal device to conduct this is a choice of flexibility and does not amount to using a personal device to conduct official council business.

Your password will need to be changed upon first logon, equally there will be specific requirements as to the composition of your chosen password for security purposes. The password (Active Directory) will need to be changed every 60 days.

Any equipment provided by the Council must not be used for illegal purposes or in any way which could bring the Council into disrepute and must not be used to operate a private business.

The Council Member must not allow any unauthorised person to access the Council's systems using their network credentials or equipment and must keep all passwords secure. For more information on good practice on password control, please refer to Appendix A.

It should be noted that anything stored locally on Council equipment, explicitly, not on the network drives or OneDrive is not backed up by the Council. Members must only save documents to their U drive or OneDrive. Saving files to the desktop is prohibited.

3.0 Hardware Issued by the Authority

All ICT equipment, applications and data belong to and remain the property of the Council.

ICT equipment will be expected to be used for all democratic work, including use at Council meetings and reading/annotating agendas, reports, minutes and accessing SDDC emails.

The Member will take all reasonable steps to ensure ICT equipment is kept secure and protected from theft/damage. Particular care should be taken with regard to ensure ICT equipment is not left on view in cars or on public transport etc.

The Member will grant access to ICT equipment to any authorised employee or agent of the Council at reasonable times for the purpose of service, repair or audit.

If a Member ceases to be a Member of the Council, all equipment must be returned to the Council within 10 working days.

The storage or processing of personal data (e.g. details of names and addresses) may be unlawful in certain circumstances, advice is available from the Data Protection Officer or the Elected Member Data Protection Handbook.

Malfunctions with the ICT equipment should be reported to the ICT Service desk on 01283 387500. Under no circumstances should arrangements be organised for third party repairs to be undertaken.

Members should only use the following number to report or seek help for technical issues (01283 387500). This number is monitored continuously through operating hours. Members should not contact any officer on another number unless they have arranged this separately. This is in place to ensure Members receive a standardised and auditable service on each interaction.

In the event of damage to any part of the equipment, you should inform the ICT Service Desk immediately on (01283 387500).

In the event of theft or loss of ICT equipment the Member must report the incident to the Police to obtain a crime reference\lost property number and then provide this information to the ICT Service Desk on (01283 387500).

In respect of hardware issued for external connection to the Authority, the Council will insure and keep insured the hardware concerned.

In the event of the installed virus protection software discovering a virus on the hardware, you should follow the virus procedure as laid out below:-

Reporting the Action on Finding a Virus

- If a Member suspects a virus is affecting the operation of software and/or hardware, they shall switch off the hardware affected. Phone the ICT Service Desk immediately, who will advise what action to take.
- Do not try to ignore the fact that a virus may be affecting your files – it will not clear itself and will continue to infect other software files/hardware, and potentially other users of the network.

4.0 Internet Usage and External E-Mail

Any Member accessing the Internet for search/browsing or e-mail must ensure they adhere to the following rules:

- Do not access any websites that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council. Websites visited by any user (Member or officer) when connected to the Council server are recorded, monitored and will be available for audit, if necessary.

- If you accidentally enter any area which could be construed as unfit, obscene or inappropriate you must leave it immediately and inform the ICT Service Desk. Be aware that your computer records which sites you have accessed.

- Care must be taken when downloading files via the Internet. Computer viruses may be contained in files and/or e-mails and can severely damage the operation of the laptop. If the installed virus protection software detects any viruses, please follow the instructions on the previous page.

- If you receive unsolicited e-mail (e.g. junk or chain mail), do not forward such items to other recipients.
- Never leave the computer unattended whilst you are using the Internet. The session will be your responsibility. It should also be noted, the computer should not be left switched on and unattended for security purposes.

- E-mail guidelines and Internet guidelines are attached at Appendices B and C respectively.

5.0 Use and Care of the Equipment

All ICT equipment and system access supplied to you is primarily for your use relating to official Council duties.

Examples include:-

- Communicating with officers, other Members, MPs, government officials, partner organisations and where appropriate members of the public.
- Dealing with official Council correspondence.
- Communicating and obtaining information in support of approved personal training and development activities.
- Viewing and obtaining material for discussion by a political group on the Council, as long as that relates to the work of the Council and not the political party.
- Formulating policy and the decision-making process of the Council or other organisation on which you have been formally appointed to represent the Council.

5.1 Use for Party Political Purposes/Party Political Publicity

Under the Members' Code of Conduct, there is an absolute restriction on Members using, or authorising the use by others, the resources of the Council ('resources' includes land, premises and any equipment such as PCs, laptops, copiers, scanners, printers, paper and software and the time, skills and help of anyone employed by the Council) for political purposes.

There is also a clear statutory ban on the use of Council property for any purpose connected with party political publicity, either at election time or at any other time. Publicity is defined as any communication, in whatever form, addressed to the public at large or to a section of the public. This will include press releases and letters to the media.

At election time there are also detailed restrictions on the use of Council property for other party political purposes as well as publicity. The safest course is to avoid the use of Council ICT equipment for any purely party political purpose at any time.

This includes all the work you do in connection with:-

- Constituency party meetings, Ward party meetings etc. or communications to party members collectively in their capacity as party members.
- Processing names and addresses of your constituents for electioneering purposes.

5.2 Personal and Casework Use.

As explained in section 2 of this policy, Members typically have three roles. It is important to distinguish between these roles to ensure compliance with Council policy. It is strongly recommended when undertaking casework to use @southderbyshire.gov.uk communication channel and corporate device.

Members are permitted to communicate with the Council in relation to their casework on personal email addresses however it must be noted the risk for data in transit and the sharing of data collected in this capacity is the responsibility of the Member not the Council.

If a Member uses personal email accounts to conduct casework they are the sole data controller and will be responsible for reporting any data incidents to the ICO. If a Member uses their @southderbyshire.gov.uk email account the Council will at that point become an independent data controller with responsibility to keep data collected by the Member safe on the Council's network.

The use of personal email addresses (or third party addresses such as a work account) is strictly prohibited in relation to the sharing or discussion of internal affairs, such as confidential information, Council documents or any communication not intended for the public domain and you should use your South Derbyshire email account as your primary channel for these purposes.

The ICT equipment or services may be used for personal or casework purposes provided that:-

- It is not detrimental to corporate interests
- It does not cause any disruption, disturbance, inconvenience or degradation of the service
- It does not interfere with the work of the Council
- It does not involve unacceptable use of the Council's system
- The setup of the equipment and connection is not changed in any way

5.3 Examples of unacceptable use

- Breach of confidentiality
- Breach of security rules/guidelines, e.g. breaking through security controls
- Representing values which are contrary to any Council policy
- Promoting any private or personal interests such as selling personal possessions, property or promoting a social activity not related to the Council
- Deliberate accessing or attempting to access, viewing, downloading, displaying, printing or distributing from the internet of what is considered to be material likely to incite criminal behaviour
- Using or transmitting abusive, defamatory, libellous, profane or offensive language
- The importation of computer viruses and similar software through unauthorised downloading of files and programmes from external sources
- Running software that is not approved by the Council
- Loading software applications directly onto any of the Council's systems without approval
- Knowingly causing congestion and disruption of networks and systems
- Deliberate accessing or attempting to access, viewing, downloading, displaying, printing or distributing of what is considered to be offensive, obscene, sexually explicit or pornographic from the internet
- Sending e-mail messages and/or attachments that cause offence or are considered to be harassment on the grounds of gender, race, ethnic or national origin, disability, family status, age, religious belief, class or sexuality. Examples are messages that contain sexual innuendoes, racially biased jokes or obscene language.
- Using mobile data cards for personal use
- The use of proxy sites.

This is not an exhaustive list.

5.4 Monitoring of Communications

You need to be aware that the Council has the capability to monitor all use of the internet and intranet and logs and retains the records.

The reason that monitoring takes place is to ensure that the standards and rules set by the Council and legislation are complied with. This is also in place in relation to managing data security incidents.

We record or monitor:-

- Details of websites visited or attempted to be visited
- Pages accessed
- Files downloaded
- Graphic images examined
- Any file attachments (e.g. pictures or word documents)

The Council has the capability to monitor, log and retain e-mail correspondence.

Any potential viruses within e-mail and internet traffic passing through or outside the Council's systems are scanned for.

5.5 General Issues

Any messages or information you send to someone outside the Council, or statements that reflect on the Council (this is either in a personal capacity or on business use through an electronic network such as on-line services or the internet) wherever appropriate you must make it clear that the views expressed are personal and may not necessarily reflect those of South Derbyshire District Council.

You must not use anonymous mailing services to conceal your identity when mailing through the internet, falsify e-mails to make them appear to originate from someone else.

5.6 Care of the Equipment

Members are required to take all reasonable care of the Authority's equipment. Members should not eat, drink or smoke over the equipment.

Lending ICT equipment to any third party is strictly forbidden

Members should never attempt to delete software packages from ICT equipment. It should be noted that these will be updated or changed over time and ICT can do this remotely.

Members can only connect their ICT equipment to their home or third party Wi-Fi networks when using the Corporate VPN.

Do not subject the ICT equipment to extreme heat, cold or moisture (do not store in vehicles).

When carrying ICT equipment in a vehicle or on public transport every effort should be made to keep the device secure i.e. do not leave on display.

The whereabouts of the ICT equipment should be known at all times. It is the users responsibility to keep their equipment safe and secure.

One charger will be issued with each item of ICT equipment. If lost Members will be expected to replace these at their own cost.

5.7 Strictly forbidden Activity

Illegal installation transmission of copyright materials.

Members are not allowed to send, access, upload, download, or distribute offensive, profane, threatening, pornographic, obscene, or sexually explicit materials. Downloading other browsers is not permitted. Proxy sites are also prohibited.

Use of South Derbyshire District Council District Council's internet/E-mail accounts for financial or commercial gain or for any illegal activity.

5.8 Malfunction of Equipment

Malfunction or any other technical problem with ICT equipment should be reported to the ICT service desk 5705 (01283 387500), under no circumstances should repairs be organised without consultation with ICT.

5.9 Cameras

Members must use good judgement to ensure the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.

If a Member would like to use a camera in meeting for photos or videos they should raise their intent with the meeting chair.

5.10 Social Media

ICT equipment provided to Members should not be used to access personal social media sites such as Facebook and Twitter. It is however permissible for Members to use equipment provided for social media for legitimate and official council business reasons such as communicating with residents or maintaining SDDC corporate sites. It is recommended that Members have separate social media accounts for personal and professional use.

5.11 Excessive Usage

ICT equipment cannot be used abroad without configuration changes. To use equipment abroad please contact the ICT service desk within 14 days of departure. Please note, to minimise security risk it is recommended not to use equipment abroad if the need isn't urgent or necessary.

Cellular data is provided to meet the business needs of the Council and appropriate usage tariffs will be selected accordingly.

The Council provides a mobile data contract which pools access to cellular network across the organisation. Each connection (sim card) is monitored for excessive use and proactive reporting is in place to stop any accidental connections incurring large overspends.

Wi-Fi connections should be used wherever possible to avoid additional usage charges. The Civic Offices (in Council Chamber & Members room) Wi-Fi will be preconfigured and equipment can easily be setup for home Wi-Fi or where this is provided in other locations such as Cafés, hotels. If assistance is required please contact ICT Services on 01283 387500.

5.12 Malicious Use/Vandalism

Any attempt to destroy hardware, software or data is forbidden. Defacing of ICT equipment, including the SDDC ID tag, in any way is prohibited (stickers, markers, etc.).

5.13 Printing

Members are only permitted to print out documents on the Council's network using a Council printer. These are located at Civic Office, Rosliston Forestry Centre, Oaklands and The Depot. This control is in place to safeguard against data loss through printing from the SDDC network to devices outside our network. Members can send a print job to a corporate printer via the laptop even if they are not at one of these locations. The job will only be released to print when the Member scans their badge on the top of the printer.

Members can also request Officers of the Council to print documents in relation to Committee meetings if they are unable to do so beforehand.

5.14 Microsoft Teams

The Council uses Microsoft Teams as its main collaboration tool. It is a communications tool which can also be used for joint working on documents and allows other collaborative functions such as task management.

Teams does not replace email in the case of formal communication of conducting business and a record of chat history is not kept. Members are encouraged to make use of Teams when contacting relevant and appropriate Officers as this in most cases is the fastest way to get a response given the complete integration of Teams in modern working practices.

5.15 Emergency Situations

In an emergency situation, the Chief Executive or other senior officer in the Council may issues an exemption to parts of this policy when responding to a major incident. This is likely to involve a balanced approach to risk and reward on any given situation and will be communicated widely at the relevant time.

6.0 The Law

6.1 Data Protection

All Officers and Members when conducting Council duties are responsible for complying with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 including any consequential data protection legislation as updated, amended or replaced from time to time which concerns the direct use of personal data, whether that information is held in electronic or paper-based form.

The Council has a statutory requirement to report Personal Data breaches to the Information Commissioners Office ("ICO") within 72 hours of becoming aware of the breach. Members must therefore report a breach (or any suspected breach) without undue delay to the Council's Monitoring Officer and Data Protection Officer. If the breach is likely to result in a high risk of adversely affecting the individual's right and freedoms, the Data Protection Officer will inform the individual.

The GDPR applies to Personal Data, meaning any information relating to an identifiable person who can be directly or indirectly identified, such as the name, identification number, location data or online identifier. It also applies to sensitive personal data such as genetic data and biometric data. For more information around Data Protection, please see the Elected Members Data Protection Handbook.

You should ensure that the Personal Data held for Council purposes should not be used for political purposes.

You should be aware that the unauthorised processing or disclosure of such data is prohibited under the GDPR, you are responsible for ensuring that there is no such unauthorised disclosure of data. If the Council fails to abide by the GDPR, it could be prosecuted and fined up to 20 million Euros (17 million pounds) or up to 4 per cent of the Council's turnover. The GDPR also imposes legal liability if you are responsible for a breach. In addition, the Council or the individual officers may be liable to pay compensation to any individual who has suffered material or non-material damage as a result of such a breach.

6.2 Computer Misuse

The Computer Misuse Act 1990 covers unauthorised or malicious use of any computer system. It is the law used to prosecute hackers and people who write and distribute computer viruses deliberately.

It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access. This law protects against employees and members of the public who deliberately cause damage to systems and data. The Act also makes it illegal for a person to deliberately delete data or sabotage systems to the detriment of the Council.

6.3 Harassment

You can commit harassment either by using e-mail or send a harassing message to someone or by downloading and distributing material from the Internet which constitutes harassment because it creates an intimidatory working environment. Harassment and discrimination are unlawful under the Protection from Harassment Act 1997 and the Equality Act 2000. As with any form of harassment under the anti-discrimination legislation, the intention of the parties is irrelevant. The problem with e-mail is that, with the lack of visual clues, offence may be caused where none was intended.

6.4 Obscene Material

Publishing legally 'obscene' material is a criminal offence under the Obscene Publications Acts 1959 and 1964. This includes electronic storing and/or transmitting obscene materials that would tend to deprave and corrupt or paedophiliac material.

6.5 Defamation or false statements

The liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the Internet will be responsible for it and liable for any damage in accordance with the Defamation Act 2013 for causing or likely to cause serious harm to the reputation of the victim.

In addition to the liability of the individual who made the libellous or false statement, the Council may also be held liable. This could be either under the normal principles of:-

- Indirect liability because the Council is considered responsible - known as 'vicarious liability'; or
- Direct liability as a publisher because of providing the link to the Internet and e-mail system.

An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

Do not put anything on an e-mail or an attachment, which you would not put in a normal letter on Council headed paper. Treat e-mail as you would a postcard going through the open post.

6.6 Copyright

Although any material placed on the Internet or in public discussion areas is generally available, the originator still has moral and, possibly, legal rights over it. You should not copy it without acknowledging the original source and, where appropriate, gaining their permission. This applies even if you modify the content to some extent. Please note that any official material placed on a website is subject to copyright laws.

Copyright laws are different for each piece of software. In general, the copyright to every piece of software run on a system is owned by whichever company or person wrote it. The Council has a legal duty to make sure sufficient licences of the correct type are present to cover the use of all software. You must be aware of these issues and make sure that the Council has correct licences for any software you are using.

6.7 Contracts

Electronic communication, such as e-mail, is generally regarded as an informal means of communication but it is, nevertheless, capable of creating or varying a contract in just the same way as a written letter. You should be careful not to create or vary a contract accidentally, always seek advice from the Legal department if you believe you are being requested to act on behalf of the Council and sign an electronic document.

6.8 Disclaimer

Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the Council. Always remember that any statement you make may still be construed as representing the Council.

7. Responsibilities

Violation of the Acceptable Use Policy may be subject to but not limited to; action under the Member Code of Conduct, repossession, removal of content.

7.1 Member

Violation of the Member ICT Policy may be subject to but not limited to; action under the Member Code of Conduct, repossession, removal of content.

- All material viewed and stored on ICT Equipment must be in accordance with the ICT protocol and values of South Derbyshire District Council.
- Users must exercise the same prohibited uses as the use of South Derbyshire District Council computers, corporate mobile devices and laptops.

7.2 Corporate ICT

- Provide SDDC supplied ICT equipment to a recognised standard build that can access the Internet and SDDC emails from the users SDDC email account.
- Ensure any incidents in relation to ICT equipment acceptable use protocol are referred to Democratic Services and support with any investigation as necessary.
- Provide support and maintenance of ICT equipment in keeping with the corporate ICT service standards.
- Providing training and instruction on use of the SDDC estate.
- Providing advice and support to staff and Members regarding ICT equipment
- Investigation of any suspected misuse of devices
- Will be responsible for the deletion of any data, email accounts and files in line with current retention protocol when a Member leaves office. If a Member wishes to retain data they have collected for casework then a request can be made to the IT helpdesk.

APPENDIX A - PASSWORD COMPOSITION

Passwords for accessing systems should be of a complex nature.

The following guidelines give information on how passwords should be created and managed to ensure their integrity and the integrity of the systems and information, which they protect.

The following best practice guidelines should followed at all times, though it is recognised that some systems may be unable to support some of the recommended guidelines, due to technical limitations.

Password Requirements

To ensure that malicious parties or programs which guess passwords have reduced chance of being successful, users should construct a password that meets the minimum criteria for each system as shown in the table below.

System / Type	Password Age	Minimum requirements	Lockout / Wipe attempts
Network Accounts and Systems which can enforce password blacklists	60 Days	8 Characters	3
SmartPhones	60 Days	8	5 attempts and then the device wipes
Members	60 Days	8 Characters	3

To make sure the password is strong users should also ensure that passwords:

- must not contain the user login name
- must not include the user's own or relative's name, employee number, national insurance number, birth date, telephone number, car licence plate or any information about him or her that could be readily learned or guessed
- should not be single words from an English dictionary or a dictionary of another language, slang, dialect or jargon with which the user has familiarity. This is true even with a number placed at the end
- are significantly different from previous passwords and password used for other systems. Do not reuse old passwords or words spelt backwards
- do not contain commonly used proper names, including the name of any fictional character or place
- do not contain any simple pattern of letters or numbers such as "12345678" or "abc123", or deliberately misspelled words

- are not displayed in work areas or any other visible place. If a user has to write their password down, they must ensure it is kept as securely as, for example, their credit card. Write down only the password, not the system it is for and if possible include a mistake. Inform ICT should this go missing
- are not e-mailed, recorded electronically, or used via the "save password" functionality which may result in a password being taken or shared
- Finally, be careful when using systems which allow users to enter a password reminder or hint; the reminder or hint must not be the user's name, password or text which clearly identifies the password (e.g. child's name) as this is a security risk, and users MUST NOT let anyone observe them when entering their password.

Password Changes

Network passwords must be used in line with the following rules:

- Passwords must be changed when a new account is created
- Passwords must be changed, as soon as possible, after a password has been compromised or after a suspected compromise
- Passwords must be changed where they are deemed to be too weak
- Passwords must be changed on direction from the Council's ICT staff
- Passwords are changed and the account deactivated when the staff member leaves the Council
- Administrator passwords should be changed whenever a member of staff leaves the Council who had administrator access.

Password Suspension

The network will permit three attempts to enter the correct User ID and password before the account is locked. Smartphones and tablets allow five attempts before wiping the device.

When an account has been suspended, it can be released by the appropriate system administrator. In the case of the network (log on) or systems managed by ICT requests for release of suspended accounts should be made via the IT Service Desk.

To reset a password for individual applications, the relevant System Owner for that system should be contacted.

Password and Account Protection

Each user is responsible for all activities originating from any of his or her username(s).

Passwords must not be shared. Users who share their passwords may have their access to the Council's networks and systems disabled, whilst investigations are carried out and management determine the course of action (disciplinary) that may be required.

NOTE: In some cases, users may be requested to share their passwords with trusted Council employee (Audit, ICT Security, HR) in order to complete a task that is critical to the Council. In this case Director approval can be sought for an exception.

Avoid writing down passwords; if passwords are to be written down they **must** be protected. Do not stick them to the equipment they unlock or leave them out in desks, notice boards or any other place

where someone may see them. If a password must be written down, keep it securely in a wallet or purse or locked in a secure container. Ideally do not keep the corresponding username with the password as this will make it harder to use if it is lost. If possible, only record part of the password. Report lost password documentation **immediately** so that unauthorised access can be blocked.

Password Construction

Creating strong passwords does not have to be difficult, try this method.

What to do	**Example**
Start with a sentence or two	Longer passwords are better than short
Remove the spaces between the words	Longerpasswordsarebetterthanshort
Add shorthand and misspell words	LingerpswdsRsafethnsht
Add length with numbers and symbols, don't always do this at the start or end.	LingerpswdsRsafethnsht1876

While this password is fairly easy to remember the number of combinations an attacker would have to check is huge. Even if an attacker can check billions of passwords a second on thousands of computers it would still take too long to find the password.

APPENDIX B – EMAIL AND INTERNET GUIDELINES

These guidelines apply equally to internal and external e-mail and act as guideline.

Never . . .

1. Use the e-mail system for knowingly doing anything illegal under English law, or for unacceptable purposes that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council.

2. Transmit sensitive information on e-mail unless you can apply appropriate encryption using the 'sensitivity' button in Outlook.

3. Abuse others - even in response to abuse directed at you.

4. Use e-mail to harass or threaten others in any way.

5. Use anonymous mailing services to conceal your identity or falsify e-mails to make them appear to originate from someone else.

6. Access anyone else's mailbox unless they have given you proxy or authorisation rights. Unauthorised access is a breach of security.

Don't . . .

7. Use the 'Reply All' function unless everyone in the original message needs to know your response.

8. Print out messages unless you really need to.

9. Send large e-mails or attachments. It's not an economical or sensible way to handle large documents and it can halt the e-mail system. It is better to put the file on the network and direct people to it. Contact ICT for assistance.

10. Create e-mail congestion by sending trivial messages or by copying e-mails to those who don't need to see them.

11. Forward confidential or restricted items on e-mail sent to you personally without the originator's permission.

Remember . . .

12. E-mails may be read by a far wider audience than originally intended, because of the ease of forwarding messages to new recipients.

13. E-mail is not guaranteed to arrive at its destination within a particular time, or at all.

15. Always put appropriate disclaimers on your messages.

16. Any advice you give on e-mail has the same legal standing as any other written advice.

17. Before sending an e-mail, ask yourself how you would feel if your message were read out in Court or disclosed under FOI.

18. Not to assume that the message has been read just because it has been sent.

Do . . .

22. Maintain your e-mail mailbox properly:-

- Access emails regularly or make sure that a re-direction is set up if you are away for more than a day.
- Only keep messages that are necessary for current business needs or need to be retained for other purposes.
- Store all e-mail messages necessary for permanent business records in your U Drive or OneDrive, according to current record retention policies.
- Delete insignificant, obsolete and unnecessary messages, return/read receipts and attachments, regularly. Clear your 'deletion' folder daily to get rid of unwanted items.

23. Make sure you use the correct address when sending mail. If the e-mail fails to reach its destination, it may be lost or fall into the wrong hands. Double-check the address when you send important messages.

24. Consider confirmation of receipt for important e-mails.

25. Reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will or should be sent.

26. Only print an e-mail if you need to for example, a hard copy for filing / legal reasons.

28. Always enter a subject title to your e-mail. Make sure that the 'subject' field of the message is meaningful. This helps everyone file and search for his or her messages more effectively.

INTERNET GUIDELINES

If you use a connection to the Internet, you must follow the requirements of these guidelines.

Never . . .

1. Use the Council's Internet access for knowingly doing anything which is illegal under English law, or the law of any other relevant country, or for unacceptable purposes such as accessing any www area that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council.

2. Use the Council's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

3. Knowingly use the Council's Internet facilities to disable or overload any computer system, network, or equipment or attempt to disable, defeat or circumvent any systems intended to protect the privacy or security of another user, including the Council's 'firewall' security systems.

Don't . . .

5. Leave Internet connections unattended.

6. Release protected information online - whether or not the release is inadvertent, it comes under all the penalties under existing data security policies and procedures.

7. Order or pay for personal goods and services using Council equipment on the Internet.

Remember . . .

8. If you accidentally access unsuitable material, you must disconnect from the site immediately and inform the senior officer in ICT Services.

Do . . .

9. Only use Internet browser software provided and configured by the Council, and only use officially provided access mechanisms.

10. Immediately report any security problems or breaches to the ICT Service Desk.

APPENDIX C – INFORMATION CLASSIFICATION

The Council's partnership working with Central Government and other national bodies and agencies has led to the exchange and sharing of information that requires protection and handling in line with the requirements of the Public Services Network and the Government Security Classifications Policy (GSCP). The GSCP describes how HM Government classifies information assets to: ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations.

Organisations which work with government have a duty to respect the confidentiality and integrity of any HMG information and data that they access, and are accountable for safeguarding assets in line with the GSCP.

Purpose and principles

The purpose of this guidance is to ensure the Council meets its obligations under the GSCP and also has appropriate controls in place to protect its own information. It reflects the following principles:

Principle One: All information that the Council collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

Principle Two: Everyone who works with the Council (including staff, members, contractors and partners) has a duty of confidentiality and a responsibility to safeguard any Council information or data that they access, irrespective of whether it is marked or not, and is must be provided with appropriate training.

Principle Three: Access to sensitive information must be granted on the basis of a genuine "need to know" and subject to an appropriate personnel security control.

Principle Four: Assets received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

Classification / Categorisation of the Council's Information Assets

The GSCP classifies HMG information assets into three types: OFFICIAL, SECRET and TOP SECRET.

The Council operates exclusively at OFFICIAL level and the previous classifications, RESTRICTED, PROTECTED and UNCLASSIFIED no longer apply.

The main theme of the new Government policy is, at OFFICIAL at least, personal responsibility for the data you transmit, handle or store, no longer relying on security markings. This is particularly important because the UNCLASSIFED marking no longer exists.

OFFICIAL information

The OFFICIAL level covers the variety of information handled and created by the Council of differing value and sensitivity and different consequences resulting from loss of compromise.

Some of the Council's information is particularly sensitive and could have more damaging consequences (for individuals, the Council or partner) if it were lost, stolen or published in the media

This sensitive information will attract additional controls to ensure that it is only accessed by those with a "need to know". Such information should be treated as OFFICIAL–SENSITIVE.

Guidance on what information should be treated as OFFICIAL–SENSITIVE and how it should be handled appears below.

It is important to note that within the GSCP, CONFIDENTIAL is not a recognised security classification; therefore care must be taken if marking documents as confidential. It must be clear to the recipient of the information what this means and what handling requirements are to be applied.

Marking OFFICIAL information

There is no requirement to explicitly mark routine OFFICIAL information.

Security markings previously applied to council information which now fall in the OFFICIAL classification can therefore be removed.

Handling OFFICIAL information

All Council information must be:

- Handled with care to avoid loss, damage or inappropriate access.
- Shared responsibly, for business purposes, and using appropriately assured channels if required (e.g. Secure email).
- Stored securely when not in use. For example, with clear desk policies and screens locking when ICT is left unattended.
- Protected in transit and not left unattended when taken out of the office.
- Stored securely when taken out of the office. For example in a locked briefcase or locked cabinet.
- Protected to prevent overlooking or inadvertent access when working remotely or in public places.
- Discussed with appropriate discretion when in public or over the telephone. Details of sensitive material should be kept to a minimum.
- Emailed, faxed and sent by letter only to named recipients at known addresses.
- Destroyed in a way that makes access unlikely. More sensitive assets should be returned to the office for secure disposal where appropriate.

Special Instructions when handling personal data

The General Data Protection Regulations requires the Council to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk pf processing personal data.

Whilst personal data will generally fall in the OFFICIAL classification, additional controls must be observed to ensure that the Council complies with its obligations under the Data Protection Act.

- Original certificates (e.g. birth certificates, medical records, passports) should be transferred / returned by Tracked Courier;
- Multiple and restricted lists (e.g. names and addresses) should be sent by Tracked Courier and if held on electronic media, strong encryption should be used with a strong password (see Password Policy);
- Paper records containing personal data must be kept secure when off-site in a lockable case and totally separate from valuable items such as laptops;
- Partnership arrangements where electronic files of personal data are transferred should be by secure electronic methods only and encrypted except for Public Services Network.
- An individual's personal data may be sent by normal email where they have given the Council permission to send via this channel, else use secure email. The individual must also acknowledge that we cannot be held responsible if a 3rd party gains the information after the Council has sent it;
- It is the senders responsibility to ensure that the recipient's email address is correct and the receiver is ready to handle the information being sent in the required format. Specific care must be taken to ensure that personal data is not sent to recipients on a contacts list;
- When printing personal data, check that all print jobs that start are completed. Where jobs cannot complete (e.g. owing to a printer error) ensure that they are deleted from the print queue. Failure to do this could result in the print job resuming in their absence, and result in personal data being left out on the printer;
- When printing personal data, the document must be removed from the printer immediately. Personal data must never be printed to a printer accessible to the public unless the secure print facility is used;
- All unwanted printed material containing personal data must be shredded.

For any advice please contact the Data Protection Officer or ICT Service Desk.

OFFICIAL-SENSITIVE information

OFFICIAL-SENSITIVE is not a separate classification; it is simply a tool to identify OFFICIAL information that is particularly sensitivity and needs additional controls.

OFFICIAL-SENSITIVE should be used by exception and in limited circumstances where there is a clear and justifiable reason to reinforce the "need to know." This would be when compromise or loss of the information could have particularly damaging consequences for an individual (or group of individuals), a partner, or the Council.

Some examples of OFFICIAL-SENSITIVE information are as follows:

- the most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to members on contentious and very sensitive issues;
- commercial information e.g. contract negotiations that may be damage/undermine the Council or commercial partner's negotiating position if improperly accessed;
- information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- sensitive personal data;
- legal advice and information created in connection with legal proceedings.

Determining whether information is OFFICIAL-SENSITIVE

The originator of the information is responsible for determining the appropriate classification for any assets they create, with reference to this Policy, and marking the asset where OFFICIAL-SENSITIVE.

The originator must understand the business value and sensitivity of the information they create. Information should not be regarded as OFFICIAL-SENSITIVE as a matter of routine as applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls. However, not applying the OFFICIAL-SENSITIVE marking to sensitive assets may result in inappropriate controls and potentially put them at greater risk of compromise.

Responsibility for any change in the classification lies with the originator. Recipients must not re-classify a document without the agreement of the originator. Where that agreement cannot be obtained, for example because the originator no longer works for the Council, agreement must be obtained from the originator's manager.

Marking OFFICIAL-SENSITIVE information

When sending emails where interception could compromise the freedoms of recipients or data subjects an additional level of security can be added to the email via Outlook. This action will mark the email as OFFICAL-SENSITIVE.

A user should click on the 'Sensitivity' button in a new message and selecting 'Official -Sensitive'. Note, this will change how the email is received and will require the recipient to take an extra step in order to read the message.

For assistance on secure electronic transmission of files please contact the ICT service desk.