Members ICT Protocol

St.Helens Council

Version: 5.0

Version Control

Date	Version	Comments
07/02/2017	DRAFT 5.0	
16/05/2018	5.0	Approved by Council

Table of Contents

1 Introduction 3
2 Support for IT problems and lost ICT Equipment 3
3 Guidance: Information Security and IT Network Security 4
3.1 Information Security 4
3.2 IT Network Security 4
4 Member Responsibilities - ICT Equipment 5
4.1 General: 5
4.2 Password Authentication: 5
4.3 Protecting your device: 5
4.4 Mobile connectivity 6
4.5 Removable Media 6
4.6 Personal Use: 6
4.7 Use of Mobile Devices Abroad 7
5 Guidance: Online Participation, Internet and Email 7
5.1 General 7
5.2 Online Participation Principles 7
5.3 Defamation 8
5.4 Tainting of Decision Making through Biased/Closed Minds 8
6 Member Responsibilities - Online Participation, Internet and Email 9
6.1 General Responsibilities applying to all forms of Online Participation 9
6.2 Internet and Email 9
6.3 Council Website and Your Councillor Webpage 10
6.4 Social Media 11
7 Data Protection and Freedom of Information 11
7.1 The Information Commissioner's Office 11
7.2 Data Protection 11
7.3 Notification and Use of Personal Data 11
*7.4 Data Protection Principles ..... **Error! Bookmark not defined.***
7.5 Freedom of Information 12
Appendix A: Declaration 13

1 Introduction

1.1 St Helens Council will provide you with ICT equipment to enable you to undertake your duties as an elected member. You will normally be offered:

a) a tablet computer to access: e-mail, electronic papers for council meetings, calendar, documents, applications and council systems; and

b) a smartphone for: voice, text messaging, email, applications and data tethering.

1.2 In addition, you may have retained an existing local authority issued desktop / laptop computer, broadband connection or been issued with a printer for your occasional printing needs.

1.3 This Protocol sets out both guidance and your responsibilities to minimise the risk to both you and the Council, in respect of the following areas:

a) Information Security in respect of handling both official Council and personal information.

b) Your responsibilities in respect of using local authority issued ICT equipment.

c) Online participation - the appropriate use of email, internet, social media and the restrictions on the use of your Council hosted webpage.

d) Your responsibilities under data protection and freedom of information legislation.

1.1.3 This Protocol should be read in conjunction with Code of Conduct for Elected and Co-opted Members which can be viewed in Part 5 of the Constitution. Failure to comply with this Protocol may constitute a breach of the Code of Conduct.

1.4 As a condition of being provided with ICT equipment, you must comply with the terms of this Protocol and sign the undertaking at Appendix A.

2 Support for IT problems and lost ICT Equipment

2.1 If you experience a problem, with your Council issued ICT equipment, you should contact the IT Service Desk on **01744 676525** (8.00am to 5.15pm, Monday-Friday) or log a call via IT Service Desk Portal.

2.2 If your device is damaged, lost or stolen you must contact the IT Service Desk immediately on **01744 676525**.

2.3 If your device contains a data SIM card, and your device is lost or stolen outside normal office hours, then you should contact Telefonica (O_2) direct on **0844 826 0288.** Telefonica will terminate the connection on your device. Please record any reference number provided by Telefonica (O_2) and report the matter to the IT Service Desk on the next available working day.

3 Guidance: Data Security and IT Network Security

3.1 Data Security

3.1.1 The Council has a duty to protect the data it collects, in particular the personal information it holds in respect of residents and service users. The Council must comply with data protection legislation.

3.1.2 A data breach (whereby personal data is lost, stolen or disclosed inappropriately) has the potential to cause widespread reputational damage to an organisation.

3.1.3 The Information Commissioner's Office (ICO) has wide ranging powers to investigate breaches of data protection legislation, including the power to fine Data Controllers and Data Processors. *[Further information concerning the role of the ICO and your responsibilities under data protection legislation are contained in section 7 below]*.

3.1.4 It is everyone's responsibility to remain vigilant to risks associated with failing to maintain security of data. As such, care should be taken when dealing with data to consider the impact that a breach may have on either you, the Council and/or data subjects. You should take particular care with regard to electronic communication and data, such as email and social media, and ensure that Council data is not stored outside the Council's IT network.

3.2 IT Network Security

3.2.1 The extension of mobile technology and the rise in cybercrime increases the risks for all organisations to protect the data that it holds. Mobile devices, such as tablet and smartphones, provide additional security vulnerabilities due to their portability and the way that data is transmitted remotely over wireless networks.

3.2.2 As an elected member you will have access to the Council's computer network. The Council must ensure that it has adequate controls in place to ensure that only authorised users have access to the computer network and the information contained within it.

3.2.3 The Public Services Network (PSN), which enables the council to communicate securely with central and local government, places further restrictions on how computer devices are set up and are able to connect to a local authority's computer network. The Council is subject to an annual audit to ensure that it complies with these requirements. You are provided with devices that have been locked down in accordance with these requirements.

3.2.4 All computers that communicate outside of a network, e.g. via the internet or email, are subject to additional security vulnerabilities. Viruses and malware software can make equipment inoperable, destroy data or allow an unscrupulous hacker to take control of a computer and the information contained within it.

3.2.5 The Council has installed an internet firewall to ensure the safety and security of its network and information. All internet and email access is recorded, logged and interrogated for performance and capacity monitoring purposes and to ensure compliance with policies and procedures. The monitoring of an individual's usage will only be undertaken by authorised officers as part of a formal investigation into allegations of misuse.

3.2.6 All incoming emails are scanned for viruses and malware and an email filtering system has been put in place to ensure that only emails that satisfy set criteria, including appropriate content, are passed through to the Council's email system. Emails are retained for a period of two years.

4 Member Responsibilities - ICT Equipment

4.1 General:

4.1.1 ICT equipment is provided to you to facilitate your official functions as an elected member and will remain the property of the local authority. You are responsible for its safe custody and its return on ceasing to be a member.

4.1.2 Tablet and smartphones will be provided with an appropriate voice and / or data allowance to enable you to undertake your official duties. Any additional charges generated through private use must be re-paid to the Council.

4.1.3 The Council reserves the right to inspect ICT equipment to allow for the service, maintenance or repair of equipment. You are required to give officers from Business IT access to the equipment to enable this function to be carried out either in person or remotely at a suitable convenient time.

4.1.4 You must not use the device, or permit its use, in any manner that may bring the Council or yourself into disrepute.

4.2 Password Authentication:

4.2.1 You will be required to use a strong password to access both your device and the Council's IT network. Further advice can be provided should you require assistance in creating and remembering strong passwords.

4.2.2 You must not reveal your password to anyone or write it down other than to authorised members of St. Helens Council ICT staff for the purposes of addressing your IT needs and thereafter change your password so only you know it.

4.2.3 You should avoid setting passwords that are easily guessable or that you use to access other systems and websites.

4.2.4 You should be vigilant for spoof email or website login pages which may trick a user into providing their log-in credentials.

4.2.5 If you forget your password you should contact the IT Service Desk (see section 2) to enable it to be reset. Note that the content on some devices may be wiped after a number of failed attempts, which varies depending on the device, but as a minimum is three. As such, you are strongly advised to contact the IT Service Desk prior to the third attempt. This is to prevent additional inconvenience as the device will need to be rebuilt and you will lose any information stored locally on the device.

4.2.6 If you have logged a call with Business IT for an issue to be resolved there may be exceptional occasions when Business IT may need to reset your password to complete the work. You will be advised of this and notified of the password. Once the work has been completed you will be required to reset your password.

4.3 Protecting your device:

4.3.1 You should take adequate precautions to protect the device from theft or damage and lock your screen when it is not in use.

4.3.2 You must notify the IT Service Desk (01744) 676525 immediately of the loss or theft of any equipment (see section 2). This will enable the Council to either track or remotely wipe the device to protect unauthorised access to any data held upon it.

4.3.3 You should not remove or disable any equipment or software unless notified to do so by Business IT.

4.3.4 To prevent viruses and copyright implications, you are restricted from installing unauthorised software on your device.

4.3.5 The charging of your mobile device should be by way of the charger provided direct into the electric mains or appropriate car charger. You should not charge your device using the USB port attached to an untrusted computer.

4.4 Mobile connectivity

4.4.1 Data tariffs are provided on mobile devices to enable you to access data remotely and securely.

4.4.2 In addition, you can connect your device to trusted Wi-Fi networks, including Council supplied Wi-Fi and your password protected home broadband.

4.4.3 You should apply extreme caution when joining other (untrusted) Wi-Fi sources such as those found in cafes, bars and other retail outlets. Unscrupulous providers or hackers, posing as a legitimate Wi-Fi hotspot, may be able to intercept data between your device and its final destination. You should take appropriate precautions to ensure that you are only connecting to a trusted Wi-Fi network. It is recommended that Wi-Fi connectivity is routinely turned off to prevent you in-advertently joining an untrusted network.

4.4.4 You should be mindful that there are significant security vulnerabilities with using short-range connectivity products, such as Bluetooth, Air Drop or pairing, particularly within public places. Such vulnerabilities can allow hackers to eavesdrop on conversations, access data traffic or apply a virus or malicious code to a device when the functionality is switched on.

4.5 Removable Media

4.5.1 It is the Council's policy to prohibit the use of all removable media devices (e.g. USB drives, CD's, SD cards) to store data. Exceptions will be considered on a case by case basis and will be subject to a valid business case and compliance with the following requirements:

a) Only council issued encrypted removable media devices should be used.

b) The use of non-council devices is prohibited and must never be used to store Council information or be connected to Council owned IT equipment.

c) If the use of removable media has been approved, you should ensure that a scan of the device is carried out using the Council's approved anti-virus software.

d) Removable media should never be the only place where information is stored

e) Care should be taken to physically protect the device from loss, theft or damage.

f) Removable media devices that are no longer required or have become damaged must be returned to the Democratic Services Manager who will arrange for their secure disposal.

4.6 Personal Use:

4.6.1 You may use the device for appropriate personal use.

4.6.2 Any additional charges generated through private use must be re-paid to the Council.

4.6.3 You may download applications onto your Council provided tablet or smartphone from the St Helens Apps Store. Requests for the inclusion of additional apps should be made via the Democratic Services Manager.

4.6.4 You may set up a personal email account on your mobile device using an email client downloaded from the St Helens App Store. You are however prevented from using the device's own email client for creating additional and/or personal accounts, as this feature is exclusively set up for official email only.

4.6.5 Personal email accounts must not be used for Council business

4.7 Use of Mobile Devices Abroad

4.7.1 The usage of Council issued smartphones and tablet devices abroad should be for Council purposes only.

4.7.2 Data roaming will only be approved for Council business and must be agreed prior to the device being taken abroad. You should notify the IT Service Desk before you go abroad to ensure that the correct data tariff is in place.

4.7.3 To reduce unnecessary costs, you should ensure that 'mobile data' and 'data roaming' are switched off when not required. These options can be switched off by selecting Settings and Mobile.

4.7.4 You should take similar precautions when connecting to Wi-Fi as you would in the UK.

5 Guidance: Online Participation, Internet, Email and Social Media

5.1 General

5.1.1 Websites and social media provide many opportunities to engage and communicate with people in new and innovative ways.

5.1.2 This section provides advice in respect of the use of the internet, Council email, your Councillor webpage and the use of social media sites, blogs, 'wikis' or any other online publishing format.

5.1.3 Emails and social media posts are a quick and easy way to communicate but they are not like telephone calls or face-to-face conversations. Such content has the potential to have both a longer life span and wider audience than intended. Emails and posts have the same legal bearing as any written document and could be used in legal proceedings.

5.1.4 Care should be taken that your actions do not directly or indirectly bring the Council or yourself into disrepute. This includes posts or email you make in a personal capacity where there is a link to your role as a Councillor.

5.1.5 Although social media sites such as Facebook and Twitter are external to the Council, the way in which they are used or content that is submitted, may still lead to a breach of the Code of Conduct for elected members.

5.2 Online Participation Principles

5.2.1 Remember, you should participate in the same way as you would with other media or public forum.

Be responsible

- When using third-party websites (such as Facebook), know and follow their terms of use
- Do not publish any information which is not already in the public arena

Be credible

- Be accurate, fair, and thorough and make sure you are doing the right thing
- Be transparent
- Encourage constructive criticism and deliberation

Be Respectful

- Be polite, open and respectful
- Respect people's confidentiality
- Be cordial, honest and professional at all times

Be consistent

- Wherever possible, align online participation with other offline communications
- When you make a reference, link back to the source where possible

Be professional

- Be mindful that what you publish may be public for a long time
- Think before you publish

5.3 Defamation

5.3.1 You must not use online participation to publish defamatory statements or material. Anyone who believes that a member has defamed them will be able to take legal action directly against the member concerned. The relevant legislation is the Defamation Act 1996.

5.3.2 A defamatory statement is one that causes an adverse effect on a person's reputation. It must be published to a third person and refer to the defamed individual. Libel, which is a form of defamation, is the publication of a statement which exposes a person to hatred ridicule or contempt, or which causes them to be shunned, or avoided or which has a tendency to injure them in their office, trade or profession in the estimation of right-thinking members of society generally.

5.4 Tainting of Decision Making through Biased/Closed Minds

5.4.1 Members who are in positions of determining quasi-judicial processes, particularly planning and licensing applications or determining the outcome of consultation exercises, must exercise care to keep an open mind on issues which he or she may be required to make decisions.

5.4.2 The use of online participation to set out a clear position on a particular issue could well provide evidence of bias based on a particular personal interest or view, or a closed mind. This would demonstrate the artificiality of the member then purporting to consider openly all issues in the determination of that matter.

5.4.3 Members must give an accurate and even-handed account of discussions or processes that lead to decisions being taken. For example, they must not give a one-sided account of the reasons for a planning application being refused.

6 Member Responsibilities - Online Participation, Internet, Email and Social Media

6.1 General Responsibilities applying to all forms of Online Participation

6.1.1 The Code of Conduct for elected members applies to online participation in the same way it does to other written or verbal communication. Councillors should comply with the general principles of the Code in what they allow others to publish.

6.1.2 Online participation must not be used in a way that brings you or the Council into disrepute.

6.1.3 Online participation must not be used for the promotion of personal financial interests or commercial ventures or personal campaigns where you are identified as being an elected member.

6.1.4 Online participation must promote equality by not discriminating unlawfully against any person. You should never use language which promotes: religious hatred, racist, sexist, homophobic, transphobic, disablist, ageist, or other unlawful discriminatory content.

6.1.5 You should not make derogatory remarks or express derogatory opinions regarding the Council, its officers or Members or communicate extreme views that could be to the detriment of the Council or its reputation.

6.1.6 You should not use online participation to harass, intimidate or bully.

6.1.7 You should treat others with respect and not to do anything that compromises the impartiality of those who work for or on behalf of the authority. You must treat Local Government Officer's recommendations or known views impartially.

6.1.8 You must not use online participation to disclose information that the Council has considered in an exempt session, or which they are on notice is confidential for any other reason.

6.1.9 You must not publish content that may result in actions for defamation or other claims for damages (see section 5.3)

6.1.10 You must not process or publish personal data other than for the purpose stated at the time of capture (see section 7.2 - Data Protection).

6.2 Internet and Email

6.2.1 Your council Internet and email account is provided to assist you to fulfill your duties as an elected member. You must not create, download, access, display, transmit or engage in the following using your council internet or email account:

a) Create, download, upload, display or knowingly access websites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive. ("Unsuitable" material include data, images, audio files or video files, the transmission of which is either illegal under British Law or is against the rules, essence and spirit of this and other Council policies).

[Accidental access to such internet sites should be reported to the Democratic Services Manager on ext. 3219 who will record the Members name, the date, time and site(s) accessed. This information will be reported to Internal Audit.];

b) Subscribe to, or use online gaming or betting sites;

c) Subscribe to or enter “money-making” sites or use “ money-making” programs;

d) Subscribe to, enter or use peer-to-peer networks or install software that allows the sharing of music, video or image files;

e) Run a private business;

f) Break through or disable security controls, such as hacking;

g) Participate in chain emails including, jokes or ‘joke’ chains and conversational email.

The above list gives examples of “unsuitable” usage but is neither exclusive nor exhaustive.

6.2.2 The forwarding of emails to personal email accounts presents additional information security risks to the Council and should be avoided. The Council has implemented controls to prevent the auto-forwarding of emails.

6.2.3 Emails, sent to external users, containing personal or sensitive information must be kept secure which means they should be sent using appropriate encryption. You will need to include OFFICIAL-SENSITIVE in the subject field to ensure your mail is encrypted. If the message cannot be delivered encrypted for any reason, you will receive a message delayed or undelivered notice. In these circumstances, you should re-send the message using PGP. If in doubt, please contact the Democratic Services Manager on ext. 3219 for advice

6.2.4 You should take care when receiving unsolicited email, as it could be a vehicle for introducing computer viruses. If you receive what you believe to be an unsolicited mail and are concerned or suspicious of the content you should not reply to it and report it to the Democratic Services Manager.

6.2.5 Personal use is permitted provided that:

a) all usage is governed by this document and access to internet is restricted to those sites which will not breach the Council’s policies; and

b) it does not interfere with the performance of the email system and the corporate network.

6.3 Council Website and Your Councillor Webpage

6.3.1 You may not use your Member’s page on the Council website to promote political campaigns, advocate political stances on issues, nor use the site to promote a political party or persons identified with a political party.

6.3.2 You are responsible for the content of your own online participation. For the avoidance of any doubt, the Council does not authorise or in any way sanction the publication of statements that might be construed as defamatory (see section 5.3)

6.3.3 You are only permitted to publish information in the context of your official role in respect of matters of general public interest.

6.3.4 You must not breach copyright or intellectual property rights

6.3.5 During election time (from the ‘notice of an election’ to the election itself), parts of Members’ web pages may be suspended. Visitors will still, however, be able to contact them through their web pages.

6.3.6 Members must not use the Council Website to secure personal advantage or secure use for themselves or others of the resources of the authority (for instance, by advertising a commercial service or by using the pages to encourage the Local Authority to purchase a particular item or service).

6.4 Social Media

6.4.1 The appropriate use of social media by Members is governed by the Code of Conduct for Elected Members and Co-opted Members. Supplementary guidance on the use of social media by elected members has been developed to support the effective use and management of social media and to minimise risk.

6.4.2 When using social media, either using Council or personal IT facilities, you should ensure that you do not publish anything, which may have the potential, through association, to bring the Council into disrepute, as set out in section 6.1 above.

7 Data Protection and Freedom of Information

7.1 The Information Commissioner's Office

7.1.1 The Information Commissioner's Office (ICO) is the UK's independent supervisory authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Complaints relating to Data Protection and Freedom of Information can be escalated to the ICO.

The ICO has the power to fine controllers and processors for serious infringements (breaches) of the General Data Protection Regulations (GDPR), up to:

- 2% of worldwide turnover, or 10m EUR; or
- 4% of worldwide turnover, or 20m EUR

dependent on the nature of the breach.

7.2 Data Protection

7.2.1 Elected members have a legal obligation to comply with data protection legislation, which aims to protect all personal data which is collected, processed, stored and disposed of. The data protection legislation gives enforceable rights to individuals (data subjects) and places obligations on those legal persons who control the manner and the purpose of the processing of personal data (data controllers).

7.3 Fees and Use of Personal Data

7.3.1 A person or organisation, which processes personal data, is defined as a Data Controller. Each Data Controller must pay the required fee to the ICO. Democratic Services will make arrangements to pay the required fee to the ICO on behalf of each elected member. Further information can be found on the ICO's website at www.ico.gov.uk.

7.3.2 Elected members must be aware of in which capacity they are processing personal data, by considering the context in which that information was received and processed.

a) As an elected member of the Council you may have access to and process personal data in the same way as employees. In this case the Data Controller is the Council rather than the elected member, e.g. a member of a Planning Committee. The member may have access to information in planning files for the purposes of considering whether or not the Council should proceed with a development. In this case the member is processing personal data on behalf of the Council.

Information that is held by the Council may not be used for political or representational purposes unless the individuals to whom the data relate (the data subjects) have agreed.

b) When as an elected member you represent residents of your ward, you are processing personal data in your own right, and are therefore the Data Controller. Examples include, the processing of personal data in order to timetable ward surgery appointments or progress complaints made by local residents.

This means that you are accountable for ensuring data protection legislation is adhered to.

c) When an elected member is acting on behalf of a political party, the party is the Data Controller, and the party determines how and why the personal information is processed for the purpose of their individual campaigns.

Individuals, who are not part of any political party but campaign to be an independent elected member to a particular ward, are their own Data Controller, and will need to arrange any required payment to the ICO.

7.3.3 Elected members are advised to refer to the ICO for advice and guidance for elected representatives and political parties:

https://ico.org.uk/for-organisations/political/

7.3.4 Elected members should also be familiar with the Council's Data Protection Policy.

7.4 Freedom of Information

7.4.1 The Freedom of Information Act (FOIA) gives a general right of public access to all types of recorded information held by public authorities.

7.4.2 In relation to the FOIA:

a) Elected members are not authorities for the purposes of the FOIA.

b) Correspondence between elected members or information held by an elected member for their own private, political or representative purposes will not usually be covered.

c) Information received, created or held by an elected member on behalf of the Council will be covered, for example, where an elected member is acting in an executive role as part of Cabinet. Information created or received by an elected member both in electronic or manual form will only be covered if it is held for the Council's own business.

7.4.3 Elected members are advised to read the ICO's document 'Information produced or received by Councillors':

http://ico.org.uk/~/media/documents/library/Freedom_of_Information/Detailed_specialist_guides/information_held_by_a_public_authority_for_purposes_of_foia.ashx

Appendix A: Declaration

Undertaking

I have read the Members' ICT Protocol.

I agree to be bound by the terms set out within it.

Signature:

Print Name:

Date:

2 copies of this document must be provided and signed by the Member.
1 copy to remain with the Member, the other to be retained on file by Democratic Services, Town Hall.