INFORMATION & ICT SECURITY

Elected Members – Information & ICT Security Acceptable Use Policy

Document information

Title	Information & ICT Security – Elected Members – Acceptable Use Policy
Version	V0.2
Date Created	21 November 2014
Status	Draft for consultation
Author	Ben Akins
Owner	SIRO
FOI Classification	
Review Schedule	Annually
Last Reviewed Date	n/a

Document History

Version	Date	Description	Author
0.1	21 November 2014	Original document	Ben Akins
0.2	23 December 2014	Initial Review	Mike Zammit
0.3	10 October 2016	SCOC Working Group	

Consultation Route

Recipient	Date	Feedback provided	Document updated
IT Services Team & Group Leaders and relevant Officers			
IT Services Management Team	22 December 2014	Various changes and comments	23 December 2014
Internal Audit			
HR			
Legal Services			

CONTENTS

1. INTRODUCTION 4

2. ELECTED MEMBERS, DATA PROTECTION & THE ICO 4

Data Protection Act 1998 4
Data Controllers 4
Information Commissioner's Office 4
Offences 5
Further Guidance 5

3. WHY INFORMATION SECURITY & DATA PROTECTION ARE IMPORTANT 6

Consequences 6

4. INFORMATION & ICT SECURITY AT WIRRAL COUNCIL 6

5. KEY INFORMATION & ICT SECURITY PROTOCOLS FOR MEMBERS 7

USE OF EMAIL 7
USE OF PASSWORDS 8
DATA STORAGE 8
COUNCIL EQUIPMENT 9
General 9
Smartphones & Tablets 10
INFORMATION / ICT SECURITY INCIDENTS 10
USE OF THE INTERNET 10

6. POLICY COMPLIANCE 11

7. REVIEW AND REVISION 11

APPENDIX 1 – ELECTED MEMBERS ACCEPTABLE USE POLICY - FORM 12

APPENDIX 2 – DATA PROTECTION ACT – EIGHT KEY PRINCIPLES 14

1. INTRODUCTION

1.1 The purpose of this document is to confirm your responsibilities as a new or existing Elected Member of Wirral Council in terms of the acceptable use of council information and ICT facilities.

1.2 As well as outlining your responsibilities under the Data Protection Act it also details the key policy rules you must follow to ensure the safe handling, storage and use of council and constituents' information.

1.3 It supplements the Wirral Council Members' Code of Conduct, and replaces the existing 'Use of Council Computer Facilities Code of Practice – Members' document. You must sign the form in Appendix 1 to confirm you have read, understood and accept the contents and terms and conditions of this policy.

1.4 Further information and guidance concerning information security is available on the council's intranet site – here[1].

2. ELECTED MEMBERS, DATA PROTECTION & THE ICO

2.1 Wirral Council is responsible for a wide variety of information, some of which is personal and sensitive. Additionally, as an Elected Member, you are responsible for the personal information of Wirral citizens in your constituency. You and the council have legal and moral responsibilities to ensure that the security of that information is maintained.

Data Protection Act 1998

2.2 The Data Protection Act (DPA) regulates the holding and processing of personal information that relates to living individuals.

2.3 Further information on the DPA is available here[2].

Data Controllers

2.4 All Wirral Council Elected Members are registered with the ICO as Data Controllers. A description of the processing activities of Data Controllers is placed on a public register of notifications. Data Controllers must comply with eight data protection principles (see Appendix 2) which together form a framework for the proper handling of personal information. Individuals whose personal information is processed have rights under the Act, for example, to a copy of the information that is held about them.

Information Commissioner's Office

2.5 The Information Commissioner's Office (ICO) is "the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"

2.6 It has the power to enforce penalties, including financial penalties, to organisations or individuals who have failed to comply with the requirements of the DPA. A list of organisations who have received such penalties is available here[3].

---

[1] http://wbcnet.admin.ad.wirral.gov.uk/governance-information-responsibilities/councillors-responsibilities-information

[2] https://ico.org.uk/for_organisations/data_protection

[3] https://ico.org.uk/enforcement/fines

2.7 When you, as an Elected Member, consider using personal information for any particular purpose, you should take into account the context in which that information was collected to decide whether your use of the information will be fair and lawful.

2.8 Personal information held by the council should not be used for political or representational purposes unless both the council and the individuals concerned agree. For example, it would not be possible to use a list of the users of a particular council service for electioneering purposes without their consent. An example would be using a list of library users to canvass for re-election on the grounds that the member had previously opposed the closure of local libraries.

2.9 When campaigning for election as the representative of a political party, candidates can use personal information, such as mailing lists, held by their parties. However, personal information they hold as Elected Members for casework should not be disclosed to the political party without the consent of the individual.

2.10 Candidates for election should also be aware of the requirements of the Privacy and Electronic Communication (EC Directive) Regulations 2003 that regulate unsolicited electronic marketing messages sent by telephone, fax, email or text.

2.11 When campaigning for election to an office in a political party, members should only use personal information controlled by the party if its rules allow this. It would be wrong, for instance, to use personal information which the candidate might have in their capacity as the local membership secretary, unless the party itself had sanctioned this.

Offences

2.12 The Data Protection Act contains a number of criminal offences including:

- When someone is required to notify (ie: register with the ICO) and does not do so. For example, a councillor who holds computerised records of constituents' details for casework purposes, would commit an offence if they had not notified this use of personal information.
- Making unauthorised disclosures of personal information. For example, an Elected Member who disclosed personal information held by the council to their party for electioneering purposes without the council's consent could commit an offence.
- Procuring unauthorised disclosures of personal information. For example, an elected member who obtained a copy of personal information apparently for council purposes, but in reality for their own personal use (or the use of his or her party) is likely to have committed an offence

Further Guidance

2.13 The ICO website is a source of further information and guidance for Elected Members - http://ico.org.uk/for_organisations/sector_guides/political

2.14 Additionally, the ICO have produced specific guidance - Data Protection Good Practice Note – Advice, for elected and prospective members of local authorities:

ICO Advice Elected Members

3. WHY INFORMATION SECURITY & DATA PROTECTION ARE IMPORTANT

3.1 Wirral Council maintains an Information Governance Framework which seeks to protect the security of its information assets. This is a combination of policy, procedural and technical controls which together help council officers and you, as an Elected Member, manage the risks to the confidentiality, integrity and availability of council information.

Consequences

3.2 Failure to adequately protect council or constituents' information will result in a compromise of its security which can have a number of negative consequences for you and the council, including:

- Financial penalties - The ICO can issue monetary penalties up to £500,000 to organisations which have failed to comply with the DPA.
- Legal ramifications – Serious breaches of the DPA can result in legal action, including prosecution.
- Reputational damage – Data breaches are often reported in the media and consequently result in the public perception of an organisation and/or the individuals who represent them, being damaged.
- Emotional / physical harm – The compromise of personal and sensitive data can result in harm to the individuals who the information relates to.
- Compliance – Failure to maintain information and ICT security can result in the council not complying with the Public Services Network (PSN) and NHS IG Toolkit standards. This could result in the authority being unable to deliver key services.

4. INFORMATION & ICT SECURITY AT WIRRAL COUNCIL

4.1 The controls which make up the Information Governance Framework are outlined in the Council's IG Policy. Underpinning this policy are specific policies, procedures and standards, covering:

- How the council manages information risk
- What HR-related security controls are in place
- How access to information and ICT systems is controlled
- How the security of ICT systems and equipment is maintained
- What physical security controls the council has implemented
- How information or data breaches are handled
- What information security training staff and Elected Members must complete
- Considerations when sharing information with third parties
- Secure transfer of information
- Retention and disposal of information

4.2 Additionally, the council has established key information governance roles and forums to ensure information security is continuously managed and improved. These include the establishment of the Information Governance Board and Information Governance Operational Group.

4.2.1 The authority also has a Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs) and Information Asset Administrators (IAAs), all with specific information governance responsibilities. Further information on these roles can be found in the Information Risk Management Process document.

Information Risk Management Process

5. KEY INFORMATION, ADVICE & ICT SECURITY PROTOCOLS FOR ELECTED MEMBERS

5.1 This section will provide you, as an Elected Member, with the key information and ICT security protocols you must follow to keep council and constituents' information safe. It does not provide detailed information about the specific policies and procedures referred to in section 4. Detailed documentation is available on the council intranet covering each of the policies and procedures relating to information and ICT security.

USE OF EMAIL

5.2 **Secure email must be used when sending sensitive or personal information externally** - Personal or sensitive council information could include:

- Personal information relating to individuals, particularly children or vulnerable adults,
- Financial or commercially sensitive information,
- Information which could negatively affect the council if disclosed to unauthorised individuals or organisations

5.3 Sensitive information should be sent to external email addresses from either a secure GCSx email account or a standard user@wirral.gov.uk account which has been configured to enable the sending of encrypted email. Standard user@wirral.gov.uk accounts should not be used to send personal or sensitive information externally as they are NOT secure. Further details can be found on the intranet – here.

5.4 Care should always be taken to ensure that the recipient name / email address is correct when sending sensitive information, even if it is being emailed internally, ie: to other @wirral.gov.uk accounts.

5.5 **Personal or sensitive information must never be sent by fax.**

5.6 **Internet email accounts (such as hotmail, gmail or yahoo email accounts) must not be used to send or store council information** - The forwarding of emails from @wirral.gov.uk accounts to personal email accounts (for example to work at home) is prohibited as the information is not secure in transit or at rest when stored on personal devices.

5.7 **The auto-forwarding of emails from council emails accounts to less secure accounts, including personal email accounts, is prohibited**.

5.8 **The forwarding of so-called chain emails, including joke emails, is prohibited** - as they use network and storage space and may contain viruses.

5.9 **Don't respond to suspicious emails** - Spam is the name given to bulk emails sent to a random selection of email addresses. Spam is mainly 'phishing' emails which attempt to obtain personal information such as bank details and 'pharming' emails which try to get users to click on web links to often malicious websites.

5.10 The Council has introduced measures prevent the majority of spam emails getting to users' accounts. Unfortunately the senders of these emails continue to find way of bypassing controls.

5.11 If you suspect an email is spam, or looks suspicious in nature, **DELETE IT IMMEDIATELY. DO NOT REPLY.**

USE OF PASSWORDS

5.12 **Don't share your username and password -** Under no circumstances should your username and password be used by someone else to log on to the network. If you share your login details any inappropriate activity on your account will be recorded against you.

5.13 If you think someone else knows your password, contact the IT Services Service Desk and **reset it!** If you or a colleague need access to an IT system, **apply for it!** And, most importantly, **do not log on to someone else's account**!

5.14 **Do use complex passwords and keep them safe** - Your User ID and password are the first line of defence for the Council's ICT systems. Choose a 'strong' or complex password to minimise others being able to access your account.

5.15 You must choose passwords that adhere to the following:

- Have at least seven characters.
- Have at least three different types of characters including upper case, lower case, numbers or special characters.
- Not include consecutive identical, all-numeric or all-alphabetic characters.
- Be more complex than a single word (such passwords are easier to compromise).

Tips:

- Avoid words that are exactly as they are found in the dictionary.
- Use phrases rather than words.
- Substitute other characters for letters for example: overthemoon could become 0v3r+h3m00n.
- Avoid using a password that could easily be guessed by using person-related information, such as names, telephone numbers and dates of birth

DATA STORAGE

5.16 **Don't use personal devices to connect to the council network or store council information** - Under no circumstances should personal equipment be connected to council computers or the network as this could inadvertently introduce malware, such as viruses, onto the network. Personal devices are those that are not issued by the council and include, but are not limited to:

- Laptops
- Tablet PCs
- Mobile phones (including smartphones)
- PDAs
- Digital cameras
- MP3 players
- Datasticks – access to USB ports is now restricted by default. If you need to use removable media you must complete the online INET05 form. This is available on the intranet here along with further information concerning removable media usage, such as the need to encrypt/password protect

devices such as datasticks. If you have any questions regarding removable media usage please contact the IT Services Service Desk.

5.17 **Don't store council or constituents' information on unsecure devices -** Data stored on unsecure devices (eg: unprotected removable media, laptops, tablet PCs) is at risk of being compromised if lost, stolen or damaged. Devices should be encrypted to prevent unauthorised access to any data held on them.

5.18 **Don't save council data on the local, or c:\, drive of computer devices -** All data should be saved on the council's networked drives, eg: H:\, K:\ or J:\. Data saved to the local, or C:\, drive of a computer is at risk of being lost should the device fail or be stolen. Data saved on the network is backed up by IT Services and can be recovered. Where the use of the C:\ is absolutely necessary, data should only be stored temporarily and must be uploaded back to the networked drives as soon as possible.

5.19 **Don't store personal data on council devices or the council network-** Personally data including digital photographs, music and videos, must not be stored on council devices or on locally or networked fileservers. This takes up costly storage space and can slow down network performance.

5.20 **Store and dispose of documents safely -** All documents containing confidential council information should be kept in a locked cupboard or drawer overnight. When disposing of sensitive documents, only use confidential waste bins. These are identifiable by a locked lid with a letter-box size hole in the top.

5.21 **Store mobile devices securely when not in use** - Mobile devices should not be left out in the office overnight. They should be kept in secure storage and, where possible, 'Kensington Locks' used to secure laptops to desks – these are available on the iProcurement system. If using devices at home they should not be left in sight of windows or in places which may invite an opportunist thief.

COUNCIL EQUIPMENT

General

5.22 **Do not attempt to change the configuration of council computers -** Members must not load personal software, including games, onto council computers. The hardware and configuration of the computer must not be changed. requests for changes should be directed to the IT Services Service Desk.

5.23 **Return Council IT equipment when it is no longer needed** – Council-issued IT equipment and software must be surrendered to IT Services if you cease to be an Elected Member.

5.24 **Don't share or copy software** - All software provided by the council remains the property of Wirral Council, or the licensing organisation as appropriate, and may not be shared or copied to another machine or user.

5.25 **Don't let others use your council equipment** – Council IT equipment is provided for the sole use of Elected Members primarily for council business. No person, other than the Elected Member, may use the equipment. Use by family, friends or other non-council users is not permitted.

5.26 **Don't use council equipment for party political purposes** - In accordance with the Local Government Act 1986 and the Local Authority Code of Practice on Publicity, Members should not utilise Council equipment for any party political purpose or to

publish any material which in whole or part appears to be designed to effect public support for a political party.

5.27 **Lock your computer when leaving it unattended** - When leaving a computer unattended, even for a short time, the screen must be 'locked' to prevent others accessing your account. Press 'Ctrl – Alt – Delete' at the same time and select 'Lock Computer'. On your return press 'Ctrl – Alt – Delete' at the same time and the computer will prompt you for your log in details before allowing you to access your account again.

Smartphones & Tablets

5.28 The leadership of all parties with five or more Elected Members will be offered Council provided smart phones. The term 'Leadership' is defined as the leader and deputies of the parties. All members of the Cabinet will also be offered council provided smart phones.

5.29 All Members will be offered the facility to securely access council emails from their own smart phone, provided it is on the approved list of suitable smart phones. In such cases the council's Mobile Device Management software will be installed on the device. This enforces specific security controls such as access to the device and remote wipe should the device be lost or stolen.

5.30 All Members accessing such information from council provided or personal smart phones must comply will all relevant information governance and security policies.

INFORMATION / ICT SECURITY INCIDENTS

5.31 **Report suspected information and ICT incidents** - Any event that may compromise the confidentiality, availability or integrity of council information is an 'information or ICT security incident.' This includes the disclosure of information (either deliberately or accidentally) to an unauthorised person as well as the loss of, or damage to ICT equipment used to store or process council information.

5.32 All staff and Elected Members must report information security incidents so that action can be taken and reduce the possibility of similar events occurring in future.

5.33 If you identify a security vulnerability or suspect a security incident has occurred you should:

- contact the IT Services Service Desk immediately on 0151 666 4080
- inform your party leadership

5.34 Appropriate action will then be taken depending on the nature of the incident. Further details of what you should do following a security incident are available on the intranet.

USE OF THE INTERNET

5.35 Access to the internet by Members will be routinely monitored for any unauthorised or unacceptable use. Any breach of these conditions could result in withdrawal of the equipment or in some cases a criminal prosecution.

5.36 Members are expected to demonstrate a responsible approach to the use of resources available to them, and to show consideration for other users, both those using the council's facilities and those with whom they may come into contact on the internet.

Members are expected to behave in a legal, moral and ethical fashion that is consistent with council policies and standards.

5.37 It must be recognised that any view communicated over the internet will be deemed to be the view of the council, and will in most cases be treated as equivalent to correspondence sent by traditional formal routes. Any personal view expressed via a council e-mail address should be endorsed, "The contents of this e-mail are the personal view of the author and should in no way be considered the official view of Wirral Metropolitan Borough Council".

5.38 Social Media – Members are directed to Wirral MBC Social Media Policy and LGA Guidance that may be found on the council's intranet. The ICO have published guidance on the use of social network sites and the implications for the DPA – this me be found here: https://ico.org.uk/media/about-the-ico/policies-and-procedures/1895/ico-social-media-policy.pdf

6. POLICY COMPLIANCE

6.1 Any breach of this policy, hereafter called an offence, will be subject to investigation by the Monitoring Officer of the council in consultation with Internal Audit and assisted as appropriate by technical staff. The Monitoring Officer will take action as appropriate following an investigation into the offence which may result in one or more of the following actions.

- Notification of the offence to the Party Group leader
- Notification of the offence to the Wirral MBC Standards Panel
- Notification of the offence to the Police

6.2 If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information/ICT Security Officer and/or the Monitoring Officer.

7. REVIEW AND REVISION

7.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

7.2 Policy review will be undertaken by the Information/ICT Security Officer in conjunction with the Senior Information Risk Owner and the Monitoring Officer.

APPENDIX 1 – ELECTED MEMBERS ACCEPTABLE USE POLICY - FORM

By signing this form you are confirming you have read and understood the requirements detailed in the Elected Members – Information & ICT Security Acceptable Use Policy document and you agree to abide by its requirements.

Additionally, the following activities, whilst not an exhaustive list, are unacceptable:

1. The access to or creation, transmission or publication of any illegal or indecent images, sounds, data or other material.

2. The access to or creation, transmission or publication of any data capable of being displayed or converted to such illegal or indecent sounds, data or other material

3. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience, discrimination or needless anxiety, or which may intimidate or create an atmosphere of harassment.

4. The creation, transmission or publication of defamatory material.

5. The receipt or transmission of material that infringes the copyright of another person.

6. The creation, transmission or publication of any material in violation of Data Protection legislation or of any UK or international laws or regulations. Such activity may constitute a criminal offence.

7. The transmission of unsolicited commercial or advertising material to other users of the council's network or users of the internet.

8. The deliberate unauthorised access to facilities, services, data or resources within the Council or any other network or service accessible via the Internet, or attempts to gain such access.

9. Unauthorised access to the electronic mail of another individual.

10. Deliberate activities with any of the following characteristics or that by their nature could result in:

    - wasting staff or other users' efforts or network resources
    - corrupting or destroying other users' data
    - violating the privacy of other users
    - disrupting the work of other users
    - using the Internet in a way that denies service to other users (for example by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files)
    - continuing to use any item of software or to access any material after being requested to cease its use because of disruption caused to the functioning of the Council's network or the Internet (for example utilities designed to broadcast network-wide messages)
    - the introduction or propagation of malware.

11. Where the internet is being used to access another network, any abuse of the acceptable use policy of that network.

12. Any use of the internet or other facilities that could damage the reputation of the Council.

13. Any breach of this policy, hereafter called an offence, will be subject to investigation by the Monitoring Officer of the Council in consultation with Audit and assisted as appropriate by technical staff. The Monitoring Officer will take action as appropriate following an investigation into the offence which may result in one or more of the following actions.

- Notification of the offence to the party group leader
- Notification of the offence to the Standards Board for England
- Notification of the offence to the Police

Issued to:

……..

Date:

……..

I agree to abide by the terms defined above

Signed :

……

Date:

……

A signed copy of this document should be returned to the Head of Democratic Services with a copy held by the individual Elected Member.

APPENDIX 2 – DATA PROTECTION ACT – EIGHT KEY PRINCIPLES

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.