**Appendix 2**

**West Dunbartonshire Council**

**(Information Security Policy Framework)**

**Acceptable Use Policy (AUP)**

## Contents

## 1. What is the Policy for?

1.1. West Dunbartonshire Council ('the Council') recognises the benefits of Information and Communications Technology (ICT) and encourages the use of ICT equipment, systems and services in all aspects of its business. Whilst all the varying technology stacks and enabling technologies are essential for new ways of working, it is important to have clear policies on ICT use to minimise existing and emerging risks.

1.2. This policy supports the Council's commitment to Information Security and forms part of this wider framework of documents which include;

- WDC Information Security Policy;
- Acquisition and Disposal of ICT;
- Privacy and Monitoring;
- Information Security DPA forum Charter;
- Reporting of Information Security Concerns; and

Related documents such as

- Social Media Policy & Guidance;
- Discplinary policy;
- Information Handling and Classification procedure (under development); and
- Records Management guidance.

1.3. Due to the pace of technology change and new threat emergence, it is not possible to have specific guidance for all eventualities. In such cases, where no specific guideline / policy guidance exists and where the risk is deemed high, then direction on breaches or suspicious activity is raised with senior management and/or ICT immediately and by any and all means available.

1.4. This policy supports the Council's Code of Conduct, the overriding principles of which apply at all times.

## 2. Who is this Policy for?

2.1. This policy and its framework applies to all users who have access to ICT resources provided by the Council, meaning all

- Employees
- Elected Members
- Agency workers
- Contractors / Subcontractors (subject to any relevant provision in their contracts)
- Employees of trusts, agencies and companies that use the Council's ICT resources
- Students and volunteers (where undertaking work experience or similar
- Partner organisations
- Any other person(s), without exception, who uses or requires access to Council owned or leased ICT equipment, systems and networks

2.2. All users of the public access network for Libraries or WDC Wi-Fi have separate guidelines covering acceptable terms and conditions of use

2.3. For the purposes of this Policy, ICT Resources means all elements of the Council's ICT Infrastructure, comprising (but not limited to):

- Data Network and main computer systems;
- Kiosks, Tills, Virtual reality devices, imaging equipment and video conferencing facilities;
- Telephones, Mobile phones and any hosted voice systems;
- PC's and portable computers (e.g. laptops, notebooks, tablets, and mobile / smart devices);
- Peripheral computer equipment (e.g. printers, scanners, Multi Function Devices, external drives and portable media);
- Software and any other services (including email and the Internet) accessed through any of the above; and
- Data and information assets accessed through any of the above (regardless of where they are location, processed or communicated).

## 3. Why do we need this Policy?

3.1. It is important that the use of ICT resources is regulated, to ensure that the Council complies with the relevant legislation, regulatory codes of practice and its own corporate governance requirements, equal opportunities and anti-discriminatory policies and ICT best practice. The Council has developed this Acceptable Use Policy (AUP) to set standards and provide users with clear instruction and guidance on what constitutes acceptable and unacceptable use.

3.2. It is important that all Users have a shared understanding of what acceptable use is and are confident in using ICT Resources in line with the Council's values and behaviours and in accordance with the Employee Code of Conduct (for Council Employees) and the Elected Member Code of Conduct (for Elected Members) and in accordance with the terms of this policy. This clarity and shared understanding helps protect the Council and its assets from damage or loss as a result of deliberate or accidental behavior. It helps to ensure that all West Dunbartonshire Council information, particularly personal, customer and business sensitive information, is treated securely and appropriately at all times and ensure that all information collection, processing and sharing activities are identified and managed.

3.3. This AUP forms part of the framework for procedures and guidance relating to information processing, management, protection and handling. It provides guidance on acceptable use for all formats of information, systems and processes used. It ensures that the Council has a clear policy in place for the acceptable use of ICT resources and complies with the relevant legislation, regulatory codes of practice and its own corporate governance requirements.

3.4. It is important to state that if individual users have concerns about their ability to comply with this policy that they must NOT logon or use ICT resources and they should raise their concerns with their Line Manager. All such concerns must be resolved to the Council's satisfaction with affected users then being prepared to accept he Council's terms and conditions of this policy before proceeding further.

## 4. What do I need to be aware of?

4.1. Users must take all reasonable steps to comply with this Policy and should endeavour to ensure that all ICT resources are used effectively, safely and securely and that all

reasonable precautions are taken to avoid loss, theft and damage.

4.2. All persons covered by the scope of this policy should maintain an awareness of all the associated framework documents referenced in section 1.2 above.

4.3. Responsibility for maintaining awareness of the Council's Information Security Policy and associated framework lies with individual employees and can be located on the Councils Intranet.

4.4. All Users of the Council's ICT systems and or/services are expected to comply with this policy when making use of the Council's ICT resources. It should be understood that logging onto the Council's data networks and devices is intended to signify acceptance of this policy.

4.5. ICT are developing a new annual MOT process for portable devices, this process will require that these devices are brought to a Council location annually for healthchecks and rebuilds where appropriate.

4.6. All users of this policy must ensure portable devices are logged on to the Council network in a council location at least monthly to pull down security patches.

4.7. All users of this policy must be aware that they should not create Council-related websites without agreement from the WDC Web Manager

4.8. All users must lock their device when they leave it unattended.

## 5. What is Acceptable/Unacceptable and Personal Use?

5.1. Acceptable Use

The Council defines acceptable use as the use of Council ICT resources, systems and networks in support of carrying its business and/or functions, or any other permitted activity highlighted by this Policy. This includes official Trade Union business, Council sponsored training or education services and limited personal use. The following criteria will be used, where relevant, to assess whether usage is acceptable:

- Whether usage is in support of business and service needs consistent with Council policies including those detailed at 1.2 above;
- Whether usage is in support of an individuals approved duties/remit;
- Whether usage is consistent with the Council policy, procedure and guidance that is appropriate to any system or network being used/accessed;
- Whether the handling of the information is appropriate for the type of information; and
- Whether usage is limited personal use as defined below.

5.2. Personal Use

5.2.1 ICT Resources may be used for limited personal use provided that:

- This is not associated with monetary reward;
- It is undertaken on the users own time (non-work hours eg Lunch break, before or after work);
- It does not interfere with the delivery of Council services; and
- It does not violate this or any other Council policy, and is a lawful activity.

5.2.2 The Council accepts no liability for any loss or detriment suffered by personal use of Council ICT resources. The Council does not provide a secure transaction process system for any information passed, or purchase made, for personal use. Any personal use of Council resources to create, send, import or store personal information is done entirely at the users own risk.

5.3. Unacceptable Use

5.3.1 The effective operation of the Council's resources relies heavily on the proper conduct of all Users. The use of all ICT resources must be in compliance with all appropriate legislations, relevant Codes of Conduct and Council Policies.

5.3.2 Users must only use ICT resources that have been authorised for their use. Any attempt to gain unauthorised access to any ICT resources provided by the Council or use of the Councils ICT resources to gain unauthorised access to any other systems may be a breach of this policy, and may also be a breach of legislation (including the Computer Misuse Act 1990). Only hardware and software that has been authorised for use by ICT services may be used or connected within/to the ICT network.

5.3.3 Remote Access must be only undertaken via the Council's authorised solution and authentication must be via the approved Multi Factor Authentication (MFA) solution. Any devices using these processes will be deemed to be authorised devices.

5.3.4 For a list of examples of unacceptable uses of Council ICT resources please refer to section 12 of this policy. Users should be aware that this is not an exhaustive list, and each potential breach of this Policy will be assessed on its own individual circumstances and in line with the Council policies set out at 1.2 above.

5.3.5 If a user is in any doubt as to what constitutes acceptable or unacceptable use then they should seek clarification from their line manager in the first instance.

5.3.6 Unacceptable use by Council employees may lead to disciplinary action as set out at 9. below.

## 6. What do I need to do about Information Security?

6.1. WDC recognises that information is one of the Council's most important assets and that the consequences can be extremely serious should it be lost, stolen, compromised or misused. To this end, Regulatory Services are developing a separate procedure which provides specific guidance on how to maintain the confidentiality, integrity and availability of all information processed or retained. However some guidance is available as part of the Data Protection guidance.

## 7. What does a Line Manager Need to Be Aware of?

7.1. It is Line Manager's responsibility to:

- Advise via HR system and processes of new employees, and those leaving the Council to ensure continued access to information assets and systems remains applicable with access to ICT Resources being granted on the basis of a business justification and removed when no longer needed;
- Notify ICT via ICT Service Desk self service portal of changes to folder and system access where an employee changes job / role (both outgoing and new line manager may require to undertake this);
- Any exceptions to the above must be logged via the ICT Service Desk;
- Employees reporting to them are made aware of this Policy;

- Ensure that their team and relevant suppliers/contractors (i.e. suppliers / contractors consuming WDC ICT Services ) are asked to review the policy annually as a minimum;
- Understand the risks presented by account sharing and nominate a named individual the task of monitoring use of any generic email accounts or other ICT resources. This involves the service area maintaining a log of who used the ICT resource and when it was used; and
- Report breaches or suspicious activity immediately and by any and all means available.

## 8. What about Privacy and Monitoring?

8.1 The Council seeks to safeguard users of ICT resources from inappropriate activities and unacceptable material. One of these safeguards is monitoring, others include a suite of defensive measures throughout the WDC network. All Council resources may be monitored for compliance with current legislation and Council Policies. Monitoring also has the following purposes:

- Comply with regulatory and statutory obligations;
- Monitor standards of performance;
- Ensure the effective operation of Council systems and information processing;
- Prevent or detect unauthorised use or other threats to information processing systems;
- Investigate allegations of misconduct, breach of contract, a criminal or civil offence or fraud by the user or any third party;
- Ensure compliance with Council policies and procedures;
- Review usage; and
- Ensure business operates during employee absence and other business requirements.

8.2. It may sometimes prove necessary for ICT systems to be accessed by Council management, nominated representatives and / or the Police (in particular circumstances) and for the contents of an employee's ICT account to be examined. The Council reserves the right to do this.

8.3. Monitoring will be undertaken in accordance with the Council's Privacy and Monitoring policy.

## 9. What about Breach Reporting & Consequences of Misuse?

9.1. It is vital that all users of council IT resources read and understand the policy and acquaint themselves with the framework for areas which affect them.

9.2. Breaches or suspicious activity must be reported immediately and by any and all means available.

9.3. This Policy and its framework are designed to avoid potential disciplinary action through a lack of understanding of what is acceptable use.

9.4. Breach of this policy may damage the reputation of the Council, citizens and its employees and may result in disciplinary action, criminal proceedings or disclosing information to law enforcement agencies or other third parties.

9.5. The Council may, at its sole discretion, suspend or terminate ICT access, withdraw, or remove any material uploaded by the user in contravention of this Policy.

9.6. Serious breaches of this policy may amount to gross misconduct and as indicated in the Council's Disciplinary Policy may lead to dismissal. Some examples include

- accessing another users' account;
- unauthorised editing and/or sharing of data;
- accessing or using pornographic or other indecent or obscene material;
- participating in any form of electronic communications based harassment; or
- using council equipment to facilitate illegal activity.

9.7. In the event of an allegation of unacceptable use of a Council IT Resource by a user not directly employed by the Council being upheld, the Council may ask the relevant third party (employer, 3rd Party Organisation) to take appropriate action and/or may report the matter to the Police with a view to commencing criminal investigation. These users will be subject to the provisions in the contract held with them or other acceptable use agreement they have entered into with the Council. In the event of any misuse they will be subject to the same processes as identified above.

## 10. Clarification of Policy

10.1 In the event of an issue arising from an interpretation of the AUP or framework content clarification should be sought from the ICT Security Officer in the first instance either by email or by telephoning 01389 737568.

## 11. Version Awareness

11.1 The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available on the Council Intranet. Those to whom this policy applies are responsible for familiarising themselves periodically (minimum annually) the latest version and for complying with the policy and its framework at all time.

## 12. Examples of Unacceptable Use

12.1 The following examples apply to the use of any ICT network operated by the Council (eg MOB network, wifi, telephony, wired) any Council ICT devices connected. It also includes the Council's partner organisations (HSCP, Leisure Trust, Valuation Joint Board) and Council suppliers.

12.2 It is unacceptable for an Employee to use, submit, publish, display, download or transmit (including the sharing of links or attachments) any information which:

- Restricts or inhibits other users from using the system or impairs the efficiency of the ICT systems;
- Violates or infringes upon the rights of any other person(s), including the right to privacy;
- Is offensive, indecent or obscene, including images containing nudity or sexually explicit content;
- Can reasonably be considered to promote any form of deception, defamation, racism, discrimination, harassment, maliciousness, misrepresentation, racism, victimisation, intolerance or violence;
- Encourages the use of controlled substances or uses the system with criminal intent;
- Uses the system for any other illegal purposes; and
- Breaches legislation or statutory requirements which the Council has to comply with e.g. Copyright Designs & Patents Act 1988, Data Protection Act 1998.

12.3 It is unacceptable for an Employee to use the facilities and capabilities of the Council's ICT systems to:

- Conduct any non-approved business;
- Download or install any unauthorised software;
- Undertake any activities detrimental to the Council;
- Transmit material or information or software in violation of any local, national or international law;
- Undertake, plan or encourage any illegal activities;
- Deliberately contribute to websites that advocate illegal activity;
- Harass an individual, group of individuals or organisations;
- Make offensive or derogatory remarks about anybody on discussion forums or Social Media as per the Council's Social Media Policy;
- Post offensive, obscene or derogatory content (including photographs, images, commentary, videos or audio) on discussion forums or Social Media;
- Create or share any content which breaches confidentiality;
- Transmit Spam (electronic junk mail) on Council network or Forward/Auto forward Council information to personal email addresses in line with Council's data handling policy;
- Attempt to compromise ICT equipment, systems and networks, prevent legitimate access to them, delete data, damage them or seek to cause degradation of performance or a denial of service;
- View, transmit, copy, download or produce material which infringes the copyright of another person or organisation;
- Conduct any unauthorised political activities; and
- Click email links without previously checking the source.

12.4 It is unacceptable to use ICT Resources that have been identified as having security vulnerabilities. This will be subject to investigation and development of an action plan.

12.5 Most assets are tagged to identify them as council property - these tags must not be removed or interfered with.

12.6 Employees should ensure that they do not in any way prejudice the reputation of the Council by using assets in a way which may cause embarrassment to the Council, bring it into disrepute or exposure to legal liability.

12.7 Employees must not save non-business related material to the Council's IT servers, local drives or cloud repositories, even during acceptable personal activity, e.g., personal files such as word processing, spreadsheets, PDF's etc., MP3 files (music), exe files (games, screensavers or software), jpg or mpg files (pictures or videos).

12.8 Employees must not connect **personal or unauthorised** devices with the ability to store data to Council IT equipment or networks. This includes devices such as smart phones, MP3 players and USB sticks.

12.9 Individually allocated assets such as IT accounts must not be shared with others unless a business requirement has been identified and approved, once risk assessed, by ICT Security.

12.10 Employees must refrain from the use of unauthorised on line chat rooms.

12.11 Employees must not use or attempt to access on line gambling sites or apps from council resources.

12.12 Council resources used inside or outside the work place must always be locked when unattended.

12.13 As a result of the increased risk of compromise, new processes will be developed for any council resources used abroad, this may involve the surrendering of such devices for examination prior to being reconnected to the councils networks. This may include smart phones, laptops and tablet devices.

12.14 All council provided resources must be returned to the council on request.

12.15 Employees must not disable protective software such as antivirus nor attempt to circumvent Council electronic security measures.

12.16 Users must not attempt to access blocked web sites by any measures such as proxy avoidance tools.

12.17 Employees accessing personal/sensitive data must not request access to use the BYOD facility, this includes those accessing or handling information from DWP, SCRA, Social Work, failure to comply with this control may result in a breach of Sharing agreements and/or Memorandum's on understanding.

12.18 Under no circumstances should anyone handling payment card information process any transactions from outside the controlled work place environment, failure to comply with this measure will result in a breach of the Payment Card Industry Data Security Standards (PCI DSS).

12.19 Employees must not attempt to deliberately access physical resources / facilities for which they don't have authority to access including other users accounts.

12.20 Employees must not access another users' account or undertake in the unauthorised editing and/or sharing of data.

12.21 Passwords must be used to protect all systems and must be maintained securely and not disclosed to others