East Renfrewshire Council

Acceptable Use Policy (AUP)

Contents

1. Introduction

1.1. This policy supports the Council's commitment to information security and is supported by a framework of related guidelines specific to acceptable operating practice. Where there is no specific guideline direction must be sought from line management.

1.2. It further supports the Councils Information Security Policy which aims to protect information assets and systems owned and used by the Council from threats, whether internal or external.

1.3. The Council recognises that information and IT facilities play an essential role in the delivery of services and are critical to effective and efficient delivery and operation of services by the Council.

1.4. In order to ensure that the Council can have confidence in its information, and that will be available when it is needed, information and the IT systems used for processing must be used, managed and secured appropriately.

1.5. The Council provides secure IT systems, applications and communication tools for use by staff undertaking their duties and as such these systems, applications, file stores etc. should be used for business purposes. Personal owned equipment, systems and applications (such as personal email) must not be used to conduct Council business. The AUP framework provides limited exemptions to this however when processing personal identifiable information Council provided facilities must be used.

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

2. Scope

2.1. This policy and its framework applies to all users of council assets including employees, elected members, contractors, consultants, temporary agency staff, modern apprentice, students, volunteers and personnel affiliated with third parties.

2.2. Individuals using the schools network and public access through libraries have separate guidelines covering acceptable terms and conditions of use. Elected Members have separate guidelines covering various aspects of conditions of use. Acceptable use of administrator privileges given to IT staff is managed through the IT Security Policy.

2.3. Individuals not directly employed by the Council (e.g. Consultants, temporary agency staff) are not governed by the Council's Code of Conduct. However, the Council requires that these individuals agree to adopt the principles of this Policy on the basis that it is designed to:

- comply with various legislative obligations
- protect users against claims of unprofessional action
- protect the Council's reputation and assets

2.4. "IT Facilities" refers to any IT provided equipment and systems such as: physical hardware, software applications, peripherals and components of the Councils network infrastructure that support the transmission of electronic data.

2.5. These guidelines extend to the use of all such equipment or systems. This applies regardless of where those equipment or systems are located. This also applies regardless of the physical location where user access or connections originate.

3. Awareness

3.1. Responsibility for ensuing awareness of the Acceptable use Policy and its framework can be located on the Councils Intranet:

 Refer to Acceptable use Policy Framework Awareness

4. Purpose

4.1. The key objectives of this Policy are:

- To provide clarity about the general principles the Council has defined to help protect its assets from damage or loss as a result of deliberate or accidental behaviour.
- To provide the framework for procedures and guidance relating to information processing, management, protection and handling;
- To provide a framework of acceptable use for all formats of information, systems and processes used;
- To ensure that all East Renfrewshire Council information, particularly personal, customer and business sensitive information, is treated securely and appropriately at all times;
- To ensure that all information collection, processing and sharing activities are identified and managed;
- To promote compliance with all relevant legislation and regulations regarding Council information assets.

5. AUP Supporting Frameworks

5.1. This policy is supported by a framework of guidelines that personnel, and any other party must comply with, as appropriate to the work or role being undertaken and include guidelines related to acceptable limited personal use.

 Refer to Acceptable use Policy Framework

5.2. This policy is supported by an Information Management and Classification framework of policies and procedures that personnel, and any other party must comply with, to ensure the continued protection of Council information assets.

 Refer to Information Classification, Management and Handling

6. Information Security

6.1. Individuals with access to Council information, have an individual responsibility to ensure that information is protected and handled appropriately.

6.2. Individuals with access to Council ICT systems, applications and data stores have an individual responsibility to ensure that access to systems is protected therefore ensuring the information within remains protected.

6.3. Access to all information and systems must be restricted to those individuals who have a business need for access by the use of unique user logins and passwords. Staff must never share their user credentials and must take steps immediately to change passwords and passphrases if compromised. Staff must immediately inform their line manager if they encounter access to information that is not required by them and must not further interact with that information.

6.4. Personal information must only be collected, processed, and shared where there is a legal justification or where it is in the interest of the customer and appropriate consent has been obtained.

6.5. All information must be allocated an Information Asset Owner who is responsible for deciding how, when and why information is collected, processed, shared, retained, and destroyed. Information Asset Owners must be a senior manager.

6.6. Information Asset Owners must identify all information, within their area of responsibility, and ensure, where appropriate, that it is recorded in the Council Information Asset Register. They must also identify the classification of information.

6.7. East Renfrewshire Council will ensure that suitable information sharing agreements and protocols exist to enable Services to manage information sharing securely and appropriately, both within the Council and with external organisations.

7. Individual Responsibility

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

7.2. When logging onto the Council's corporate IT network or cloud storage (Office 365), individuals are reminded of their responsibility to comply with all Information Security and Acceptable Use Policies and encouraged to take time to read these and be reminded of their content, particularly if it has been more than 12 months since they were last read.

7.3. Individuals are personally responsible for their use of Council assets. Individuals are expected to use such assets in accordance with the terms of this policy and associated framework guidelines. In cases of uncertainty, individuals should confirm in advance the appropriateness of their proposed use with their line manager.

7.4. ICT Services will periodically apply application and security updates to equipment. These must not be interfered. To assist with the continued good health of equipment PCs and laptops should be fully powered down at the end of each working day.

7.5. The sending and storage of information relating to a living individual is subject to the terms of the Data Protection Act 2018 and the General Data Protection Regulation. Employees, and other users should ensure that they respect the Data Protection Principles in their use of all Council assets.

7.6. Employees must be aware that non personal information may be subject to disclosure under the terms of the Freedom of Information (Scotland) Act 2002.

7.7. Users 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.

7.8. 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).

7.9. Employees must not connect personal 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.

7.10. Overall responsibility for ensuring assets are not misused lies with Line Managers however where assets are allocated to an individual personally (e.g. laptops, phones, usb sticks, IT accounts, access to data), individuals must accept these on the understanding that this responsibility lies with them.

7.11. 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 a line manager.

7.12. Individuals must obtain prior permission from their Line Manager before they use Council equipment for personal development or study purposes.

7.13. Council information must only be retained locally on computing equipment and peripherals that are encrypted. Encryption products must be authorised by IT Services.

8. Line management responsibility

8.1. Line Managers advise IT Service Desk of new employees, staff moving positions internally and those leaving the Council to ensure continued access to information assets and systems remains applicable with access to assets being granted on the basis of a business justification and removed when no longer needed.

8.2. Line Managers ensure that user account access to systems is periodically audited to ensure user accounts remain valid.

8.3. Employees reporting to them are made aware of this Policy at their induction or within a reasonable period of commencing employment with the Council and are annually reminded of its existence.

8.4. They regularly familiarise themselves with the terms of this policy and its framework.

8.5. Understand the risks presented by account sharing.

8.6. Ensure data storage undertaken by staff supports the council's responsibility to provide responses to Freedom of Information and Data Protection requests.

8.7. Breaches or suspicious activity is reported to Senior Management immediately.

8.8. A named individual is assigned the task of monitoring use of shared assets (e.g., a generic email account).

8.9. Line managers must ensure staff comply with all information security training requirements.

 Refer to Information Security Training Requirements

9. Privacy & Monitoring

9.1. The Council, and its service providers log and audit the use of networks, information, computers and systems. This includes email, internet, instant messaging, web conferencing, Office 365 (all components), and other use of internal and external systems. Backup files may be kept recording this usage.

9.2. With good cause, the Council may monitor, record and report on the contents of computer systems and applications, electronic files, internet use, instant messages and email messages sent, received and stored.

9.3. The Councils Privacy and Monitoring Guidelines provide information related to the monitoring of IT communications and use of IT technology.

 Refer to Privacy and Monitoring Guidelines

10. Breach of Policy

10.1. This Policy and its framework is designed to avoid potential disciplinary action through a lack of understanding of acceptable use. It is vital that all users of council assets read the policy and acquaint themselves with the framework for areas which affect them.

10.2. Any breach of this policy may result in harming the reputation of the Council and its employees and may result in disciplinary action or criminal proceedings.

10.3. Any suspected breach of this Policy will be subject to investigation and possible action in terms of the Council's Disciplinary Policy and Procedures.

10.4. Serious breaches of this policy e.g. unauthorised accessing of another users account, unauthorised editing and/or sharing of data, accessing or otherwise 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 may amount to gross misconduct and as indicated in the Council's Disciplinary Policy may lead to dismissal.

10.5. In the event of an allegation of unacceptable use of a Council asset by a user not directly employed by the Council being upheld, the Council may ask the relevant third party employers to take appropriate action and/or may report the matter to the Police with a view to commencing criminal investigation.

11. Clarification of Policy

11.1. In the event of an issue arising from an interpretation of the AUP or framework content clarification should be sought from the Information Security and Digital Risk Officer in the first instance either by email or by telephoning 0141 577 3644.

12. Version Awareness

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 with the latest version and for complying with the policy and its framework at all time.