Agenda Item No. 11

South Ayrshire Council

Report by Head of Finance and ICT
to South Ayrshire Council
of 29 June 2022

Subject: ICT Security and ICT Acceptable Use Policies

---

1. Purpose

1.1 The purpose of this report is to seek Members' approval of revisions to the Council's ICT Security Policy, which describes how ICT will apply strong governance to reduce risk to the Council, and the Acceptable Use Policy which governs the appropriate and effective use of ICT services and facilities

2. Recommendation

2.1 It is recommended that the Council:

2.1.1 approves the revised ICT Security Policy (attached as Appendix 1); and

2.1.2 approves the revised ICT Acceptable Use Policy (attached as Appendix 2).

3. Background

3.1 South Ayrshire Council has a responsibility to maintain its ICT network in a safe and effective operational state to ensure the confidentiality, integrity and availability of Council information.

3.2 The purpose of the ICT Security Policy is to describe how ICT will apply strong governance intended to reduce risk across the Council and it sets out the mandatory actions or rules that give formal policies support and direction.

3.3 South Ayrshire Council also provides access to a range of ICT services and facilities which are vital for delivery of services. To ensure the appropriate and effective use of these, it has developed policies, procedures and guidance to cover all aspects of computer use, including email, internet and monitoring.

3.4 Collectively these polices are known as an Acceptable Use Policy (AUP) and they provide practical guidance and rules on the use of ICT across the Council.

3.5 Previously the AUP consisted of a single overarching policy definition supplemented by four specific policy rules governing computer use, email, internet and the monitoring of ICT use. These have now been streamlined and revised into a single document attached as Appendix 2 for review and approval.

3.6 The last revision to the Council's ICT Security Policy was in 2017 with the Acceptable Use Policy revised in 2019. Both policies require some minor changes to reflect the accelerating pace of change in the use and application of technology including home working and the cyber threat environment that the Council operates in.

3.7 The changes are aimed at improving the currency and relevance of both policies and reflect changes recommended to the Integrity Group by ICT over the intervening two years since the previous Policy was approved.

3.8 The revised policies also commit ICT to a yearly review of both the ICT Security Policy and AUP to ensure its continued relevance across the organisation.

4. Proposals

4.1 Members are asked to approve both documents that comprise the revised ICT Security Policy (attached as Appendix 1) and Acceptable Use Policy (attached as Appendix 2).

4.2 The updates/changes to the previous version of the documents are highlighted in bold text throughout both Appendix 1 and 2.

4.3 Subject to approval, both Policies will be published on The Core, and will also be notified to employees by way of the Communications bulletin.

4.4 ICT and Public Affairs will also look at other ways of communicating this important policy to staff including videos and inclusion in both the staff induction process and the Council's annual cyber training exercise.

5. Legal and Procurement Implications

5.1 There are no legal implications arising from this report.

5.2 There are no procurement implications arising from this report.

6. Financial Implications

6.1 Not applicable.

7. Human Resources Implications

7.1 Not applicable.

8. Risk

8.1 ***Risk Implications of Adopting the Recommendations***

8.1.1 There are no risks associated with adopting the recommendations.

8.2/

8.2 ***Risk Implications of Rejecting the Recommendations***

8.2.1 Without having clear, up-to-date policies in place to govern information and cyber security the Council's overall security posture would be weakened. This would directly contribute to an increased risk for the Council from either a data/information breach or a cyber-security incident with the associated cost and reputational impacts either of these would bring.

9. Equalities

9.1 The proposals in this report have been assessed through the Equality Impact Assessment Scoping process. There are no significant potential positive or negative equality impacts of agreeing the recommendations and therefore an Equalities Impact Assessment is not required. A copy of the Equalities Scoping Assessment is attached as Appendix 3.

10. Sustainable Development Implications

10.1 ***Considering Strategic Environmental Assessment (SEA)*** - This report does not propose or seek approval for a plan, policy, programme or strategy or document otherwise described which could be considered to constitute a plan, programme, policy or strategy.

11. Options Appraisal

11.1 An options appraisal has not been carried out in relation to the subject matter of this report.

12. Link to Council Plan

12.1 The matters referred to in this report contribute to Commitment 1 of the Council Plan: Fair and Effective Leadership/ Leadership that promotes fairness.

13. Results of Consultation

13.1 There has been no public consultation on the contents of this report.

13.2 Consultation has taken place with Councillor Ian Davis, Portfolio Holder for Finance, Human Resources and ICT, and the contents of this report reflect any feedback provided.

14. Next Steps for Decision Tracking Purposes

14.1 If the recommendations above are approved by Members, the Head of Finance and ICT will ensure that all necessary steps are taken to ensure full implementation of the decision within the following timescales, with the completion status reported to the Cabinet in the 'Council and Cabinet Decision Log' at each of its meetings until such time as the decision is fully implemented:

Implementation	*Due date*	*Managed by*
Revised Policies to be published and notified to employees	31 July 2022	Service Lead – ICT Enterprise Architecture

Background Papers **None**

Person to Contact

Tim Baulk, Head of Finance and ICT
County Buildings, Wellington Square, Ayr, KA7 1DR
Phone 01292 612620
E-mail tim.baulk@south-ayrshire.gov.uk

Stewart McCall, Service Lead – ICT Enterprise Architecture
County Buildings, Wellington Square, Ayr, KA7 1DR
Phone 01292 612733
E-mail stewart.mccall@south-ayrshire.gov.uk

Date: 21 June 2022

Appendix 1

Information and Communication Technology

ICT Security Policy

Employee Handbook

June 2022

RESPECTFUL • POSITIVE • SUPPORTIVE •

THE SOUTH AYRSHIRE WAY

Table of contents

Version Control

Version Number	Effective Date	Details of Revision	Responsible Person	Review Date
0.1	Jun 2022	Initial Review – ICT, Governance , Quorum Cyber and Kevin Mullin and Stewart McCall	A Yeo	

1. Introduction

The ICT Security Policy demonstrates how the ICT Security aligns with the Enterprise Architecture Principles and ICT Strategy, and the ICT Digital Strategy to embed cyber security across the enterprise.

The ICT Digital Strategy 2021-2023 commits South Ayrshire to embedding security across South Ayrshire Council and the Digital Skills Strategy identifies being safe online as an essential skill for SAC employees.

The Council's ICT security guidance and direction is framed in accordance with the National Cyber Security Centre (NCSC) guidelines, guidance from the Scottish Government, and industry best practice.

This policy works in support of the ICT Acceptable Use Policy to ensure the Council's commitment to a simpler, safer, and more efficient ICT service.

2. Purpose

The Council has a responsibility to maintain the network in a safe and effective operational state to ensure the confidentiality, integrity and availability of Council information.

The purpose of the ICT Security Policy is to describe how ICT will apply strong Governance intended to reduce risk across the Council.

3. Scope

This policy will:

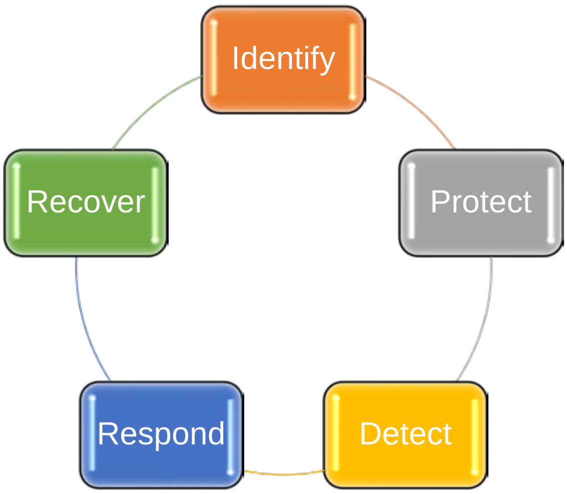
- **Define the pillars of ICT Security Governance;**
- **Provide authority for the standards that will define behaviours the Council requires in relation to ICT. ICT Security Standards are mandatory actions or rules that give formal policies support and direction; and**
- Define roles and responsibilities of employees, contractors and business partners.

4. Pillars of ICT Security Governance

Here at South Ayrshire Council, ICT (Information and communications for technology) security governance is a subset discipline of corporate governance, focused on network performance and risk management. ICT Security Governance defines how technology, people and ICT business processes ensure the Council can meet strategic and operational obligations with the minimum amount of risk.

ICT security governance enables compliance and focuses on protecting the confidentiality, integrity and availability of data and technology across the Council by ensuring the Council can identify risks and vulnerabilities, provide protection in depth, detect attacks and respond and recover with as little negative impact as possible.

It provides a foundation that ensures the Council can balance the provision of proactive ICT security safeguards with an ability to respond and recover should the worst happen.



Identify

Knowing what we have is the key to taking good care of it. Identifying and managing technology assets and electronic information is the place where security begins. This makes management of physical and data assets is a key priority for ICT. ICT is committed to delivering confidentiality, integrity and availability of electronic information and relating our security and technical solutions to reducing the risks that challenge that delivery.

Knowing where our weaknesses and vulnerabilities lie makes it possible to initiate programmes, projects and activities designed to address those vulnerabilities. An annual Security Maturity assessment will guide priorities and commitments across ICT.

Protect

The ICT Security training and awareness programme, regular system updates, business continuity/disaster recovery plans and documented policies, standards and procedures all contribute to the protection framework.

Automated and 24/7 monitoring by our managed SOC (security operations centre) provide additional protections.

Identifying risks and vulnerabilities, assessing threats, and monitoring the network continuously provides an opportunity for a proactive response. ICT is committed to taking advantage of the information gathered to improve incident response and reduce our risk levels.

Detect

The health of the network is measured and monitored regularly. Vulnerability scanning and automated alerting makes it possible to detect network issues quickly.

Employees are expected to report issues as soon as possible to ICT can take appropriate action.

Respond and Recover

The ICT incident response are intended to resume normal operation as quickly and securely as possible. ICT and ICT Security will follow agreed incident response plans. Employees are required understand their roles and responsibilities related to the incident resolution process and will participate in practice exercises when requested.

Information security incidents (breaches, threats, weaknesses or malfunctions) will be reported and investigated through the appropriate management channels using the same operational processes that are used to manage all ICT incidents.

After each incident, ICT Security will assess the residual risk and update the risk register with a plan that addresses the root cause. There will also be an investigation into lessons learned and specific continuous improvement commitments based on the discussions and resolutions.

5. The ICT Security Programme

The Council is committed to complying with legal requirements and internationally recognised information security best practices. The secure creation, sharing, storing and destruction of information in all its forms is the cornerstone of the ICT Security mandate.

People

- **Business requirements and objectives remain at the core of ICT security provision;**
- **Work with individuals and services to minimise and reduce risk and recommend secure solutions;**
- **Record and report ICT security related metrics and makes them available on the CORE;**
- **A consistent information security awareness programme with mandatory components will contribute to a strong ICT security culture.**

Process

- **Information will be protected against unauthorised access and misuse**
- **Business continuity plans and associated ICT Disaster Recovery Plans will be maintained and regularly tested;**
- **Policies, standards, processes and guidelines will be regularly reviewed and updated as necessary;**
- **Information security incidents (breaches, threats, weaknesses or malfunctions) will be recorded and investigated using a formal process;**
- **Assets and information will be classified and protected according to classification.**

Technology

- **ICT will work to continuously improve using automated processes and alerting;**
- **Changes to ICT systems and technology will be carefully controlled and approved by a Review Board prior to implementation;**
- **Regular impact and vulnerability assessments will provide a clear understanding of gaps to be addressed;**
- **A managed Security Operations Centre (SOC) will provide 24-hour monitoring.**

Risk Management and Risk Reduction

A continual risk assessment process identifies ICT security risks and then monitors, assesses, mitigates and remediates them. Risk assessments identify the risks associated with change, so we can better understand, protect and prepare for risk levels introduced by change.

Any new application, cloud service or new technology will need to undergo a risk assessment. Individuals and services will be required to initiate and participate in the ICT Security Risk Assessment process.

6. Measuring our Progress

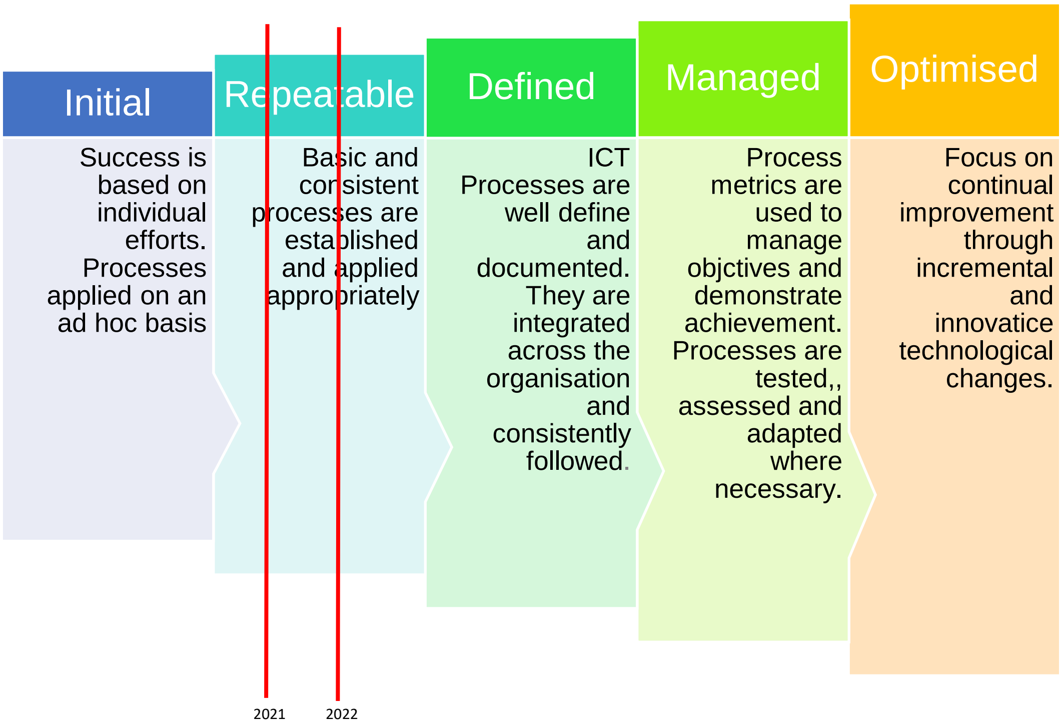
Annual Security Maturity Assessment

The managed Security Operations Centre conducts an annual security maturity review as part of its service offering. This serves as a tool for continuous improvement.

It reviews our existing cyber security controls, looking for gap areas that present an increased level of risk. We are then able to better understand our risk exposure and initiate projects and programmes that will support risk reduction across the Council.

Capability Maturity

The capability maturity model allows us to measure the maturity of information security integration with processes and behaviours across ICT. As the Council moves along the maturity scale it becomes increasingly possible to demonstrate how ICT behaviours, standards and processes are maturing to produce a culture focussed on delivering the Council's goals and objectives supported by technology centred on a documented, repeatable security foundation.



Initial

Success is based on individual efforts. Processes applied on an ad hoc basis

Repeatable

Basic and consistent processes are established and applied appropriately

Defined

ICT Processes are well define and documented. They are integrated across the organisation and consistently followed.

Managed

Process metrics are used to manage objctives and demonstrate achievement. Processes are tested,, assessed and adapted where necessary.

Optimised

Focus on continual improvement through incremental and innovative technological changes.

7. The ICT Policy Framework

The ICT Acceptable Use Policy and the ICT Security Policy

The Acceptable Use Policy seeks to promote the proper use of ICT across the Council. It provides a framework for online behaviour, information protection and risk reduction by defining individual responsibilities intended to reduce risk and make us all safer.

The ICT Security Policy partners with the Acceptable Use Policy and outlines the ICT and ICT Security commitments and contributions to risk reduction, protection and reduced exposure to known threats.

ICT Security Standards

Supporting security standards describe the goals and principles of the ICT Security Program. ICT Security Standards set out minimum acceptable requirements across three key areas: people, process and technology. Operating processes are used to define how those requirements must be carried out and guidelines are used to describe best practices and provide guidance. Standards go through a rigorous, formal review process prior to being published.

ICT Security standards exist to protect the Council and have been framed using ICT security best practices, including the recommendations of the NCSC (National Cyber Security Centre). It is the responsibility of all Council employees to understand how security standards are to be applied in the context of their specific job roles.

The following ICT security standards have been published in support of the ICT Acceptable Use Policy:

ICT Security Standards

People

- Human Resources – ICT Security
- ICT Security Training and Awareness
- Physical and Environmental Security
- BYOD and Personal Devices
- User Passphrase

Process

- Access Control
- Business Continuity - Disaster Recovery
- Change Management
- Data Classification and Retention
- Incident and Security Incident Management
- Logging, Monitoring and SOC Management
- Passphrase Management
- Risk Management
- Security Audit

Technology

- Asset Management
- Boundary Protection and Firewalls
- Platform Management / Network Management
- Portable Devices and Removable Media
- Privacy and Data Security
- Security Patch Management
- System Acquisition, Development and Maintenance
- Endpoint Protection and Remote Access

These documents are all available on the CORE. Each is supported by operational policies, processes and procedures. An annual policy/standard review ensures the documents accurately represent the ongoing requirements of the Council.

8. Responsibilities related to ICT Security

Everyone in the organisation has a role when it comes to maintaining a strong ICT Security culture.

All Employees

All employees are responsible to understand the specific cyber security responsibilities associated with their role within the Council. You must apply information classification standards and use passphrases that conform with the rules outlined in the Acceptable Use Policy and the ICT Security standard.

Individuals must understand that they are accountable for any intended or accidentally introduced vulnerability or damage to Council information systems or technology. It is necessary to advise your line manager when you no longer require permissions or access to a particular system. You may be required to participate in the assessment or review of an incident.

It is expected that you will report when something goes wrong with a device or with information that you have been using. Any suspicious or unusual ICT security related activity or any loss or damage to a Council device in your care must be reported to the Service Desk.

Also, every employee is required to participate in annual cyber awareness training.

Supervisors, Managers and Service Leads

In addition, supervisors, managers, service leads, and executive leadership are expected to maintain accurate records of users authorised to use BYOD and those who are logging in to Council systems from corporate devices.

A strong ICT security culture requires that service leads, supervisors and managers advocate for cyber security and actively participate in completing and supporting annual mandatory cyber awareness training activities.

Supervisors, Managers and Service Leads also need to:

- **Regularly review assigned permissions and request revocation of user access as required;**
- **Support employee participation in the annual mandatory ICT Training and Awareness program and actively participate;**
- **Support the digital commitments required of employees as part of the employee deal;**
- **Advice Information Governance, ICT Security and the ICT service desk of any lost or stolen data, information or computer equipment reported by an employee;**
- **Advise the ICT Service Desk of starters, leavers and individuals changing job roles within the Council to ensure smooth transition of data/information responsibilities.**

When considering or approving a purchase with an information or technology component, Service Leads must:

- **Work with ICT to ensure ICT purchases meet the defined standards;**
- **Develop supplier relationships with partners that demonstrate security standards which match or exceed our own;**
- **Use Council standards and guidelines provided by the Scottish Government when assessing the suitability of supplier contracts;**
- **Confirm appropriateness of third party and third-party subcontractors and ensure contracts contain appropriate language to reduce risk.**

In return ICT Security as part of ICT Services will commit to:

- **Ensure that the information and system resources are secured according to ICT Security standards;**
- **Provide appropriate protection at network boundaries;**
- **Apply appropriate technical controls to manage secure authentication and access to the Council's technology;**
- **Ensuring and adequate process to monitor and report unusual behaviour, and respond accordingly;**
- **Identify risks and threats and make recommendations to reduce risk;**

- **Apply the classification of data and information according to the corporate Data Classification and Retention Standard;**
- **Manage and maintain compliance activities including PCI-DSS, PSN and Cyber Essentials;**
- **Provide advice regarding ICT security within the to all services, as required;**
- **Ensure ICT Policies, Standards and processes are maintained in line with recognised security standards and industry best practice.**

9. Policy Review

This Policy will be reviewed and made available to the Integrity Group when appropriate, but no less frequently than every 12 months.

Appendix 2

Information and Communication Technology

Policy

ICT Acceptable Use

April 2022

RESPECTFUL • POSITIVE • SUPPORTIVE •

THE SOUTH AYRSHIRE WAY

Table of Contents

1. Introduction

The Council provides access to ICT facilities which are vital for delivery of services and has developed a series of policies, procedures and guidance to ensure appropriate and effective use of these facilities. The ICT Acceptable User Policy or AUP is provided for employees and covers all aspects of acceptable computer use, including email, internet use and computing equipment. A series of procedures is available on the Core in support this policy. The information in the Acceptable Use policy is based on guidance as at April 2022. The Policy has been written in line with guidance from the Council's Cyber Security specialists, the Council's cyber security partner, the Scottish Government and that published by other public agencies and authorities such as the National Cyber Security Centre (NCSC).

Anyone using the Council's equipment or network services is required to understand and comply with the ICT Acceptable Use Policy set by the Council. It is important to note that existing, new and developing technologies used in Council facilities may not be explicitly called out in this in this document but are covered by the policy.

2. Purpose

The purpose of the Acceptable Use Policy is to provide the Council's ICT users with instructions and guidance on appropriate use of information and Information and Communications Technology (ICT) equipment. It also includes the use of email, the internet, voice, and mobile IT or associated systems (e.g. printers, phones etc.). The Acceptable Use Policy supports the need of the Council to keep its ICT estate – systems, digital services, technology, networks, telephony, databases, data and other resources – in a safe and effective operational state to ensure the Confidentiality, Integrity and Availability (CIA) of the information held and processed by council services. The main objectives of this policy are to ensure:

- The Council complies with all relevant legislation including (but not limited to) the Data Protection Act 2018; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Human Rights Act 1998; the Regulation of Investigatory Powers (Scotland) Act 2000; the General Data Protection Regulation 2016; and the Privacy and Electronic Communications (EC Directive) Regulations 2003;
- ICT assets are protected in a cost-effective manner; and
- All users of ICT are aware of the responsibilities that go along with the use of Council devices, data and networking technology.

3. Scope

Employees will be offered ICT equipment and access to the Council devices, networks and data necessary to enable them to fulfil responsibilities associated with their job roles. This may include specialist tools and additional security (for example Public Services Network (PSN)). Employees are expected to contribute to the protection of these digital assets from risks posed by inappropriate use. This includes defending devices and information from unauthorised or unlawful access, accidental or deliberate loss, damage, theft, disclosure or destruction.

This policy applies to all parties (either as part of a contract of employment or third-party contract) who have access to, or use of technology assets belonging to, or under the control of the Council including:

- Elected Members (specific additional guidance is available);
- Council employees;
- Third Parties and partner organisations (specific additional guidance is available);

- Any other party using Council ICT resources.

This policy and the supporting standards should be followed when accessing Council information from any device. Questions regarding the content or application of this policy should be directed to the ICT Service Desk at *ict.servicedesk@south-ayrshire.gov.uk*.

4. Overview

The Council encourages its staff to seek innovative ways of using information technology to improve the way services are provided. The Employee Deal requires individuals to embrace new technology and take advantage of opportunities to increase digital skills. The Acceptable Use Policy provides parameters that will increase cyber awareness and contribute to reducing risks to Council assets and data.

The basic rules for all users of the Council computer network are as follows:

- A risk-based approach is used to establish the required level of security required for records, manual or electronic;
- The management of ICT and ICT Security balances risk, usability, accessibility and cost. Bypassing any security controls is unacceptable and exposes the Council to unacceptable risk;
- **Messaging apps (e.g. WhatsApp) cannot be used for performing council business or for transferring council data;**
- Where personal use of Council facilities is undertaken there can be no presumption of privacy. South Ayrshire Council electronically audits devices, internet and email usage to ensure that abuse or other issues are detected quickly;
- You should treat paper-based and electronic information with equal care. All information relating to our customers and business operations is confidential;
- In accordance with the South Ayrshire Way, equipment and information must be used in a positive, supportive, respectful way:
  - Defamatory, rude or abusive language is not permitted;
  - Communication or documents must not be used to harass, annoy or intimidate an individual or group of individuals;
  - Spreading chain mail, jokes, spam, animations or hoax virus warnings will not be tolerated;
- Where there is a breach of this policy, it is understood that the Council will take steps in accordance with the disciplinary procedures. Unlawful acts will be referred to the appropriate authorities when necessary;
- Users will not be held responsible for receiving objectionable material in unsolicited email, but must immediately upon receipt must take one of the steps listed below;
  - Refer to a line manager for an appropriate action where the email is potentially illegal or is offensive. This may then be escalated as appropriate; or
  - Immediately delete it, without forwarding it to anyone, where the email contains nothing illegal or offensive;
- A certain amount of limited and responsible personal use of our equipment is permitted.

5. Access to Council Systems

All network users will be issued a unique Username and Passphrase to be used to connect to the Council network. Individuals will be required to change the passphrase at regular intervals. Passphrases must be created, managed and protected in accordance with the *Passphrase Standard*, should not be written down, kept where others might find them or shared with anyone else including colleagues or family members. Multi-factor authentication will be required as part of the transition to M365.

Individuals will only be authorised to access systems required for their specific job roles.

It is a criminal offence under the Computer Misuse Act 1990, to deliberately attempt to access a system which you have no authority to use. ICT Services regularly monitor systems and any unauthorised attempts to access council systems will be investigated. It is also a criminal offence under privacy laws for any person to knowingly or recklessly obtain, disclose, sell or offer for sale any personal information managed by South Ayrshire Council.

All network users must agree to abide by this Acceptable Use Policy and comply with other relevant legislation.

6. Managing Digital Equipment

Changing work patterns and advancements in technology have not changed the Councils responsibility to maintain and protect digital equipment and information (official and sensitive) used to carry out council business. As users of the Council network, each of us has a responsibility to care for the device we are issued. Therefore, it is imperative to remember:

1. No attempt must be made to switch off or bypass ICT security controls, including anti-virus systems or internet controls. This applies to Council owned devices and to personal devices used for BYOD.
2. Council-owned devices may not be removed from the UK. **Exceptions can be granted for Agile Workers and Home Workers and must be approved by an Assistant Director/Head of Service;**
3. Computers and other devices owned by South Ayrshire Council are reserved for the business of the Council. Unauthorised use will be investigated under the Computer Misuse Act 1990.
4. Only authorised users will use a Council device. The Council may authorise personnel from other organisations to access Council systems by specifying acceptable usage in applicable contracts or agreements but will not issue our devices to a third-party. Third party access will not be granted until contracts or agreements are finalised and signed.
5. Adequate safeguards must be taken to protect all equipment allocated by the Council. Unsecured devices must never be left unattended. Devices must not be left on view in vehicles, public transportation or hotels and should never be left in vehicles overnight and placed away from windows to reduce risk;
6. Mobile devices (phones and tablets) must be used in accordance with the ***Portable Devices and Removable Media Standard***.
7. Caution must be exercised when browsing unfamiliar websites. Compromised websites may be used to trick users into accidentally activating malware. It is a crime under the Computer Misuse Act 1990 to deliberately introduce malicious programmes (malware or ransomware) into the council network.
8. The use of council-owned or personal computer devices for Council business, must comply with the ***Corporate Safety Standard on Display Screen Equipment***.

9. The Council cannot recover information stored on personal or corporate devices if the device is lost, damaged or stolen. Council data and information must be stored in a networked location provided for that purpose.

Council Issued Device

Based on job role requirements, the Council provides employees with technology (including laptops, tablets and smart phones) to assist in the performance of their duties. Security controls are applied to devices to protect employees, data and council infrastructure.

Use of this equipment by anyone other than the employee to whom it is issued is not permitted.

ICT is the custodian of all Council owned equipment provided to employees. All devices remain the property of the Council and must be returned in accordance with the *Device Governance standards*. Most equipment is subject to a 5-year refresh-cycle.

An employee must not use ICT equipment provided in any manner which will prevent or interfere with its primary purpose as a tool to assist in the discharge of the functions of the Council. Accordingly, the employees must not:

- Misuse or mistreat of the device provided in such a manner as to cause it to cease to function; and
- Install or use any equipment or software which may cause the computer to malfunction.

Council provided end user devices are identified by an asset tag and unique asset number. Never remove this identification.

BYOD (use of a personal device)

The Acceptable Use Policy applies to all council business conducted using a personal device registered for BYOD.

The use of Multifactor authentication will be required to increase the security when accessing Council resources from your personal device.

Support from the authority's ICT Service Desk will be limited to resolving any issues with accessing corporate information systems via personal devices. The Council cannot provide any support for an employee's own personal equipment.

Council email must not be transferred or forwarded to a personal email address.

Employees should not store Council data on their personal device – Council data must remain on the network.

7. Conducting Council Business using Technology

Employees representing the Council, virtually or online, must use the same care and attention with data and technology that they would if they were at any Council owned location or speaking to a third-party in person.

The use of social media is only available for individuals with a defined business requirement and where appropriate approvals are in place. The use of personal storage sites is not allowed, and these sites are blocked by the Council.

Employees must exercise caution when:

- Conducting any business on an unfamiliar website or cloud service;

- Registering Council email addresses on websites and apps;
- Clicking on a link within an email that has been flagged with a red banner **(Egress Defend User Guide)** indicating strong signs of phishing;
- Managing email received from unknown or unexpected sources;
- Posting messages or images on any Internet message board or other similar web-based service; or
- Working with information or images in a way that may be in violation of Copyright and Intellectual Property Rights legislation.

While using a Council device, users must not participate in any of the following:

- Illegal activity;
- Commercial or personal business activity;
- Hosting a personal website on Council owned equipment;
- On-line gambling;
- Social Networking;
- Visiting sites known to contain offensive material;
- Trolling, bullying, stalking or anti-social behaviours;
- Online dating;
- Reading or distributing obscene, pornographic, threatening, racially or sexually harassing, or in any way contravenes the Equal Opportunities policy;
- Accessing personal webmail accounts;
- Accessing personal on-line storage systems;
- Use of interactive software (such as games) across the Internet;
- Streaming films, music and podcasts using a streaming service;
- Any activity that would discredit or embarrass the Council.

Whether you are using the phone system internal to your computing device or a mobile phone supplied by the Council, there are behaviours specific to telephone use that need to be considered. The Council has the ability to track telephone calls (number called/calling and duration) and some staff members have their call interactions recorded (related to employee job roles).

The use of directory services is not allowed unless authorised by a Service Lead and use of the speaking clock is not permitted.

Employees must not call to an international or premium rate number from a council owned device or knowingly participate in telephone fraud. If you are contacted by someone attempting fraudulent telephone activity or a telephone scam you must report the call to the Service Desk.

8. Using Council Data and Information

Council data and information must be strictly controlled and protected. Compliance with the following rules will ensure you are applying appropriate protections in your effort to keep Council data and information secure.

1. Whenever the device is left unattended you must ensure information is protected by logging out or “locking” the screen.

2. Retention schemes must be followed, and housekeeping must be done to ensure the Council complies with information management requirements.

3. Council information and documents must be saved appropriately. Microsoft OneDrive is not an appropriate place to store Council data and records. To ensure Council data, documents and records are stored appropriately, Information Governance policies and M365 Governance guidelines must be followed.

4. All electronic messages including email, instant messages and chat, created and stored on Council computers or networks are the property of the Council and cannot be considered private.

5. Any personal use must be undertaken in compliance with relevant Council policies and standards. Personal use must not interfere with normal business or be detrimental to productivity.

6. Employees will not amend or delete the automatic footer that is attached to all external emails. A formal address must be included in all email, must follow the Council defined format and must not include additions.

7. Users must clearly identify any changes to another person's message before sharing it.

8. Users must never set up automatic forwarding of emails to an external email address (including a personal email address).

9. Distribution of a Council wide email must be approved by Organisational Development. This facility must only be used when the content is deemed to be of immediate interest to the majority of recipients.

10. Council data must not be held or transferred to a Flash Drive (USB Key), even as a temporary measure. See the ***Portable Devices and Removable Media Standard*** for more information.

11. Email communication with external individuals or organisations about council business can only be conducted using the provided South Ayrshire email account. A personal email must never be used for this purpose.

12. To ensure compliance with the Government's Public Services Network (PSN) Code of Connection, employees must never set up automatic forwarding of emails from their secure PSN email address to their employee email address.

13. All personal information held by the Council is subject to GDPR legislation and must be managed accordingly.

9. M365, Teams and the Cloud

The M365 Governance suite of documents are considered part of this Acceptable Use Policy as they outline how to use the new M365 tools appropriately. This suite of documents is expected to expand as our use of M365 matures. The documents can be accessed at *M365 Adoption Portal - Governance.*

The use of any new application or cloud service (a website where you need to register your details) requires a risk assessment and a data protection impact assessment (DPIA) to determine the risk and appropriateness for use within the Council. Information Security and Information Governance must be consulted before agreeing/signing up or adding any new service or technology. ICT Service Advisors will facilitate this.

Email and MS Teams chat are not Council sanctioned records management tools. Managers must ensure their employees understand the rules surrounding the classification of data and the records management procedures to be followed in every case. This may require extracting attachments and conversations and storing them more appropriately.

The use of Zoom or other online digital collaboration platforms to initiate online meetings is not authorised, but participation in calls set up by a third-party is acceptable using the web-based instance of the product.

Downloading any app that is not ICT approved onto a council device, requires a risk assessment and a data protection impact assessment (DPIA) be completed to determine the risk and appropriateness for Council tasks. ICT Service Advisors will facilitate this.

The use of a personal hosted online storage service such as personal OneDrive services, Dropbox, iCloud or Amazon is not allowed. Data stored in these services may be held in ways not allowed under the UK Data Protection law for personal data, and their use may put you in breach of law.

10. Special Considerations for Front Line Workers

Front line workers have a smaller digital footprint than employees in other environments but are not exempt from any aspect of the Acceptable Use Policy.

11. Special Considerations for Hybrid and Agile Workers

While not in a Council-owned property, Hybrid and Agile Workers will be considered Home Workers when considering the terms of acceptable use and must comply with the special considerations for home workers in addition to the base set of rules defining behaviour.

12. Special Considerations for Home Workers

Working from home can pose several unique security risks and so the following special considerations must apply when working outside a Council owned property.

You are responsible for your workspace and the safe, secure operation of your technology. Any Council owned device maintenance will be conducted at a Council owned site.

Adopt good cyber security hygiene and housekeeping practices at home to ensure council devices and information are always well protected. Remember that all actions undertaken will be attributed to you as the authorised user of the device, network and services provided by the council.

To help reduce these risks, you should ensure you carry out the following:

- **No one, not even a member of your family should have access to South Ayrshire Council's data or information. Position yourself so that your work cannot be overlooked;**
- **Do not allow family members or anyone else to use the Council owned equipment in your home for any purpose;**
- **Printing to a home printer is not supported by ICT;**
- **Connection of a council-owned device to any personal wired or wireless device is not allowed;**
- **Keep your passphrases secret, even from family members;**
- **Inform your manager as soon as possible if any sensitive paperwork or computer equipment is stolen, lost or damaged;**
- **If employees have a requirement to work from a location which is not their home (within the UK or outside the UK), they must explain the reasons for the requirement to their line**

manager and these requests must be agreed by an Assistant Director/Head of Service. These requests can only be considered for Agile or Home Workers;
- **Ensure that any work you do remotely is saved on South Ayrshire Council's network;**
- **When not in use devices should be kept out of sight and preferably locked away.**

13. Security Inspections

The Council monitors and logs the use of digital equipment, ICT services and information. Monitoring will identify individuals, the dates and times of transactions and some information about user activity. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

The Council will take measures to prevent malware from entering the Council environment. Without prior notice, the Council may need to disable or access an employee's device, email account, or network drive to remove malware. Any such access or investigation will be carried out by an appropriate and competent member of ICT under the guidance of the Information Security Team. This will be authorised by the Head of Finance and ICT.

The Council retains the right to access user electronic mail, contents of Teams meetings or Skype messages if it has reasonable grounds to do so. The Council may retrieve email or messages even though the sender and the reader have deleted them. The contents will only be accessed or disclosed for security purposes or as required by law.

Unauthorised access will be reported to the appropriate authorities.

Monitoring

To ensure information processing systems are not open to abuse, the Council reserves the right to monitor individual employee's usage. This level of monitoring must be fair and proportionate and will be appropriately authorised. By logging in to any Council information processing system or device, a user is consenting to the Council's monitoring procedures.

Monitoring is undertaken to:
- Comply with regulatory and statutory obligations, including those that guarantee privacy;
- Maintain the effectiveness of information processing systems;
- Prevent or detect unauthorised use or other threats to information processing systems;
- Prevent or detect criminal activities;
- Ensure compliance with Council policies and procedures; and
- Review usage.

Content Inspection

Employees are expected to cooperate with any reasonable security investigation.

Content inspection will only be undertaken for legitimate business reasons when necessary, including:
- Investigation of a potential cyber security breach;
- Compliance with the request of law enforcement officers;
- Compliance with legal obligations;
- Prevention or detection of activities in contravention of criminal or civil law; and
- Investigation of a potential breach of an individual's employment contract.

Content inspection may involve viewing information held in:
- Business and/or personal files and documents;

- Business and/or personal email messages or any other ICT based communication;
- Business and/or personal information displayed on a screen;
- Emails that have not yet been opened or received by the intended recipient.

14. Cyber Training and Awareness

The ICT Security Team will ensure individuals are made aware of this policy as they begin employment with the Council. The document is subject to an annual review and appropriate communication will indicate when the review period begins. The ***Acceptable Use Policy*** will be made available on the Intranet, along with the *ICT Security Policy* so individuals can reference it at any time.

Executive Managers, Service Leads and Managers must ensure this policy is followed and implemented within their area of responsibility.

Participation in the annual cyber awareness training is mandatory and employees have a responsibility to participate. Cyber resilience and lessons about good cyber hygiene will be communicated periodically throughout the year in support of this document. The cyber training and awareness programme is intended to reinforce positive behaviours and ensure employees understand the risk and vulnerabilities created by ignoring the rules outlined in this document.

Where third parties are required to access Council facilities, their responsibilities will be outlined in the appropriate agreement documentation. Acceptable use guidance documentation will be provided to third parties who require access to the Council network.

15. ICT Engagement or Notification

An employee must report any potential breach of the Acceptable Use Policy to their manager and to the ICT Service Desk with as much information as possible about the event. It is expected that any of the following will be reported immediately:

- The loss or theft of a device;
- Faults or failures on a device;
- Accidental introduction of malware, ransomware or data loss through a phishing incident;
- Warning messages generated by anti-virus software;
- Loss of sensitive data;
- Any unintended access of offensive materials in a document, email or website.

Also contact the ICT Service Desk if you use a council owned device and need to:

- Dispose of the device;
- Purchase ICT equipment or software for business use (including a cloud service);
- Install, uninstall or amend software;
- Copy Council licensed software from one device to another.

16. Compliance

All employees, and anyone who delivers services on the Council’s behalf (contractors, partners, agents or other third parties with access to the Council’s information assets) have a responsibility to comply with this policy and to promptly report any suspected or observed security breach.

Security breaches that result from a deliberate or negligent disregard of any security policy or standard may, in the Council’s absolute discretion, result in disciplinary action being taken against that employee. In the event that breaches arise from the deliberate or negligent disregard of the Council's security standard requirements by a user who is not a direct employee of the Council, the Council shall take such punitive action against that user and/or their employer as the Council in its absolute discretion deems appropriate.

ICT reserves the right to take short term preventative action which protects the Council's digital resources.

The Council may, in its absolute discretion refer the matter of any breach of the Council's security standard requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings if in the reasonable opinion of the Council such breach has or is likely to lead to the commissioning of a criminal offence.

If you don't understand the implications of this policy or how it applies to you please contact the ICT Service Desk for advice at ICT.ServiceDesk@south-ayrshire.gov.uk

17. Exceptions

A formal exception process exists to request consideration for an exception in various situations, defined in the **Exceptions Process** . Without an approved exception an individual found in breach of any standard will be investigated.

The Council may, in its absolute discretion refer the matter of any breach of the Council's security standard requirements to the police for investigation and (if appropriate) the instigation of criminal proceedings if in the reasonable opinion of the Council such breach has or is likely to lead to the commissioning of a criminal offence.

18. Legal provisions

The *Computer Misuse Act 1990* states that:

- Unauthorised access to computer-based material is punishable by up to two years in prison or a fine or both; and
- Unauthorised acts with intent to impair operation of a computer, etc. is punishable by up to 10 years in prison or a fine or both.

For example, it would a criminal offence for an individual to access a Council system just because they knew a colleague's password. This could lead to two years in prison.

The *Data Protection Act 2018* is the implementation of the UK General Data Protection Regulation (UKGDPR) and sets out what may or may not be done with personal data (that is any information that identifies a living individual). It would be contrary to UKGDPR for an individual to take home a list of citizens' names and address that might be useful to a friend in their plumbing business.

The *1988 Copyright, Designs and Patents Act* governs the use of a 'work' created by an individual or company. A "work" is defined as something that is original, created with effort and a tangible entity - an idea cannot be copyright. If a work is produced as part of employment, then the owner will normally be the employer of the individual who created the work.

It's an offence to perform any of the following acts without the consent of the copyright owner: copy the work; rent, lend the work to the public; broadcast or show the work in public; or adapt the work. For example, an individual may commit an offence by showing documents they wrote on how to manage Council procurement to a third party. It could also be an offence to copy training material that an individual found useful but is licensed for use only by the Council.

The *Equality Act 2010* legally protects people from discrimination in the workplace and in wider society. It sets out the different ways in which it's unlawful to treat someone. The Equality Act covers age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity.

Other relevant legislation:

- Civil Evidence (Scotland) Act 1988;
- Copyright (Computer Programs) Regulations 1992;
- Freedom of Information (Scotland) Act 2002 and Scottish Public Authorities Amendment Order 2020;
- Human Rights Act 1998;
- Counter Terrorism and Security Act (2015);
- Official Secrets Act 1989;
- Criminal Procedure (Scotland) Act 1995;
- Public Records (Scotland) Act 2011;
- Regulations of Investigatory Powers (Scotland) Act 2000;
- Serious Organised Crime and Police Act 2005;
- Civil Contingencies Act 2004;
- Communications Act 2003;
- The Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000; and
- Wireless Telegraphy Act 2006.

19. Policy Review

This Policy will be reviewed and made available to the Integrity Group when appropriate, but no less frequently than every 12 months.

Appendix 3

South Ayrshire Council
Equality Impact Assessment
Scoping Template

Equality Impact Assessment is a legal requirement under the Public Sector Duty to promote equality of the Equality Act 2010. Separate guidance has been developed on Equality Impact Assessment's which will guide you through the process and is available to view here: Equality Impact Assessment including Fairer Scotland Duty

Further guidance is available here: Assessing impact and the Public Sector Equality Duty: a guide for public authorities (Scotland)

The Fairer Scotland Duty ('the Duty'), Part 1 of the Equality Act 2010, came into force in Scotland from 1 April 2018. It places a legal responsibility on Councils to actively consider ('pay due regard to') how we can reduce inequalities of outcome caused by socio-economic disadvantage, when making strategic decisions. See information here: Interim Guidance for Public Bodies in respect of the Duty, was published by the Scottish Government in March 2018.

1. Policy details

Policy Title	ICT Security Policy and ICT Acceptable Use Police
Lead Officer (Name/Position/Email)	Stewart McCall, Service Lead – ICT Enterprise Architecture – stewart.mccall@south-ayrshire.gov.uk

2. Which communities, groups of people, employees or thematic groups do you think will be, or potentially could be, impacted upon by the implementation of this policy? Please indicate whether these would be positive or negative impacts

Community or Groups of People	Negative Impacts	Positive impacts
Age – men and women, girls & boys	-	-
Disability	-	-
Gender Reassignment (Trans/Transgender Identity)	-	-
Marriage or Civil Partnership	-	-
Pregnancy and Maternity	-	-
Race – people from different racial groups, (BME) ethnic minorities and Gypsy/Travellers	-	-
Religion or Belief (including lack of belief)	-	-
Sex – gender identity (issues specific to women & men or girls & boys)	-	-
Sexual Orientation – person's sexual orientation i.e. LGBT+, lesbian, gay, bi-sexual, heterosexual/straight	-	-
Thematic Groups: Health, Human Rights & Children's Rights	-	-

3. What likely impact will this policy have on people experiencing different kinds of social disadvantage? (Fairer Scotland Duty). Consideration must be given particularly to children and families.

Socio-Economic Disadvantage	Negative Impacts	Positive impacts
Low Income/Income Poverty – cannot afford to maintain regular payments such as bills, food, clothing	-	-
Low and/or no wealth – enough money to meet Basic living costs and pay bills but have no savings to deal with any unexpected spends and no provision for the future	-	-
Material Deprivation – being unable to access basic goods and services i.e. financial products like life insurance, repair/replace broken electrical goods, warm home, leisure/hobbies	-	-
Area Deprivation – where you live (rural areas), where you work (accessibility of transport)	-	-
Socio-economic Background – social class i.e. parent's education, employment and income	-	-

4. Do you have evidence or reason to believe that the policy will support the Council to:

General Duty and other Equality Themes **Consider the 'Three Key Needs' of the Equality Duty**	**Level of Negative and/or Positive Impact** **(High, Medium or Low)**
Eliminate unlawful discrimination, harassment and victimisation	Low
Advance equality of opportunity between people who share a protected characteristic and those who do not	Low
Foster good relations between people who share a protected characteristic and those who do not. (Does it tackle prejudice and promote a better understanding of equality issues?)	Low
Increase participation of particular communities or groups in public life	Low
Improve the health and wellbeing of particular communities or groups	Low
Promote the human rights of particular communities or groups	Low
Tackle deprivation faced by particular communities or groups	Low

5. Summary Assessment

Is a full Equality Impact Assessment required? (A full Equality Impact Assessment must be carried out if impacts identified as **Medium and/or High**)	~~YES~~ **NO**

Rationale for decision:

This report seeks Members' approval of revisions to the Security Policy and Acceptable Use Policy. Their decision on this has no specific equality implications

Signed : Tim Baulk **Head of Service**

Date: 19 May 2022