APPENDIX ONE

Legislation

Information security is managed in accordance with the following legislation.

The Copyright, Designs and Patents Act 1988	UK copyright law which gives creators of literary, dramatic, musical and artistic works the right to control how their material may be used.
The Computer Misuse Act 1990	This was created to criminalise unauthorised access to computer systems and to deter the more serious criminals from using a computer or the data it stores by inducing a computer to perform any function with intent to secure access. The act has been modified by the Police and Justice Act 2006.
Data Protection Legislation as defined by the Data Protection Act 2018	The main piece of legislation that governs protection of personal data in the UK. It provides a way that individuals can enforce the control of information about themselves.
Human Rights Act 1998	This act governs interception or monitoring of communications, especially article 8 which guarantees respect for an individual's private and family life, their home and correspondence. Public authorities can not interfere with these rights unless it's justifiable to do so.
Regulation of Investigatory Powers Act 2000 and Regulation of Investigatory Powers (Scotland) Act 2000	Aims to make sure that various investigatory powers available to public bodies are only exercised in accordance with the Human Rights Act 1998. The act legislates for using methods of surveillance and information gathering to help the prevention of crime and terrorism.
Electronic Communications Act 2000	Gives legal recognition for electronic signatures and makes it simpler to amend existing legislation that could hamper the development of internet services.

Telecommunications Act 2003	Governs fraudulent and improper use of telecommunications equipment

Freedom Of Information (Scotland) Act 2002	Provides the right of access to recorded information of any age held by public sector bodies in Scotland. There is a duty on all local authorities to adopt and maintain a publication scheme approved by the Scottish Information Commissioner.
The Privacy and Electronic Communication (EC Directive) Regulations 2003	Replacing the Telecommunications (Data Protection and Privacy) regulations 1999 and amendments 2000, these cover issues relating to privacy of electronic communications including telemarketing and cookies.
Public Records (Scotland) Act 2011	The council must prepare a records management plan setting out arrangements for the management of the authority's public records.

APPENDIX TWO

Standards

Information security is managed in accordance with the following standards.

STANDARD	DEFINITION
Information Technology Infrastructure Library (ITIL)	A set of concepts and techniques for managing information technology, infrastructure, development and operations.
ISO/IEC 27001 and 27002	International standards for information security management.
National Information Assurance (IA) Strategy (2007)	This outlines an approach for the UK in adopting information risk management by making sure the correct level of professionalism, education and training; availability of IA products and services as well as compliance and adoption of standards.

Payment Card Industry Data Security Standards (PCI DSS)	Standard developed by major credit card companies as a guideline to help organisations that process card payments to prevent fraud and other security vulnerabilities and threats.
Public Services Network (PSN) Code of Connection	The PSN is a private wide area network across which secure interactions between connected organisations can occur (previously known as GSX).
Security Policy Framework (SPF)	The SPF describes the principles and approaches that central government have established to protect its assets, whether they be people, infrastructure or information and at the same time assist in the delivery of public services. The SPF applies to all organisations associated with the delivery of public services.
Scottish Government (SG) Cyber Security Action Plan	The action plan, developed in partnership by the SG and the National Cyber Resilience Leaders Board (NCRLB), sets out the action the SG intends to take in order to make progress towards the 3rd outcome of the Cyber Resilience Strategy, "We have confidence in, and trust, our digital public services."
Cyber Essentials Accreditation	Accreditation against a set of basic technical controls to help organisations protect themselves against common online security threats.

APPENDIX THREE

Supporting Documents

To make sure the objectives of this policy are met all staff must comply with the following guidelines. Senior management must ensure the material is understood and adherence appropriately monitored.

- Acceptable Use Policy (including Email Guidelines and Social Media Guidelines)
- Corporate Information Security Guidelines
- Data Protection and Confidentiality Guidelines
- Information Security Incident Reporting Procedure
- Data security breach management procedure
- Mobile flexible working guidance
- Code of Conduct for Employees

Version	Purpose/change	Author	Date
0.1	First draft based on Glasgow	Wendy Barber	28.2.18
0.2	Second draft after discussion with Ian Rennie	Wendy Barber	16.3.18
0.3	With Ian Rennie's comments	Ian Rennie	
0.4	With Wendy Barber's comments	Wendy Barber	13.6.18
0.5	At meeting Wendy Barber/Ian Rennie	Wendy Barber	21.6.18
0.6	Final draft	Wendy Barber/Ian Rennie	23.1.19
0.7	Minor change to replace reference to Homeworking Policy to Mobile Flexible Working Guidance	Wendy Barber	2.4.19

Appendix 5

POLICY ON ACCEPTABLE USE OF ICT RESOURCES

1. Introduction

This document sets out our policy and guidelines on the permitted use of our Information and Communications Technology (**ICT**) resources and what action may be taken if you breach this policy. It outlines the minimum standards to be followed by users of our ICT resources. Our ICT resources includes our networks, network equipment, software, applications and IT equipment including telephones.

This policy replaces all previous versions.

2. Users

This policy applies to everyone who uses our ICT resources:

- Council and Falkirk Community Trust staff
- Elected members
- Contractors
- Consultants
- Volunteers
- Interns
- Modern apprentices and graduates
- Any other person who has access to our ICT resources.

This policy does **not** apply to:

- School pupils

3. Responsibilities

All users are required to read this policy and to comply with it at all times.

If you are a manager or supervisor, you must:

- Make sure that your staff are **aware** of this policy and have signed a **user access form** before using any of the ICT resources.
- **Authorise** use of ICT resources for your team.
- Make sure your staff **comply** with this policy when using our ICT resources.
- Deal with **breaches** of this policy (more information in section 8).
- Make sure that if you have **staff changes** – new staff starting, moving or leaving – you complete the relevant forms and send them to HR and ICT. This will allow the access rights to our ICT resources to be correctly updated for the member of staff.

4. Working arrangements

This policy applies at all times, to individuals using our ICT resources whether in our buildings, at home or when mobile working.

This policy applies to:

- PCs and thin-client devices such as I-Gels
- Telephones (including mobile and landlines)
- Mobile devices (including laptops, tablets and iPads)
- USB storage devices
- Business applications (for example MyView, Integra and the social work information system)
- Fax machines
- Our communications network
- Radio systems
- IT connected devices – Internet of Things
- Software
- IT networks

5. Guidelines on personal use of our ICT facilities

You are allowed to use our ICT resources for personal use provided it does not:

- Hinder our business
- Incur any additional cost to use
- Adversely affect the running or our systems
- Bring us into disrepute

Personal use must not:

- breach the general guidelines set out in this policy
- make use of business information which has not been made available to the public (for example our Council Tax system – access is explicitly prohibited and this would be a criminal offence under the Computer Misuse Act 1990 and Data Protection Legislation)

Personal use must not include:

- Allowing others, such as friends or family, to use our ICT resources.
- Using your business email address to subscribe to personal mailing lists and clubs
- Installing and downloading programs or apps not corporately approved
- Using file sharing programs not authorised by the Council
- Using encryption to obscure the content of personal message and files

We will not accept responsibility for:

- Storing backups of personal files
- Restoring copies of personal files from backups on request –
- Any loss you incur as a result of personal transactions made using our ICT resources.

6. General guidance on the acceptable use of our ICT resources

These guidelines apply to both business and personal use.

Software

- Software, including media files such as music and video, must only be used in accordance with licence agreements and UK copyright law. Downloading, making, using or distributing unauthorised software is illegal and is not permitted on our ICT resources.

Personal data

- You must follow our Information Security Guidelines and our Data Protection Guidelines to ensure personal data is kept secure.

Business use of social media

- Staff who use social media for business purposes will be given support and training by their manager in its appropriate use in line with our media protocols.
- If your role requires you to post updates to social media sites, remember you are representing the Council and anything you publish reflects directly on us. If you think you've made a mistake online, notify your manager immediately.
- You should use the same safeguards as you would with any other form of communication. Do not publish personal or other confidential information on social media.
- Always consider any potential risks before publishing on social media and have plans in place to mitigate them.

Personal use of social media

- Guidelines are attached to this policy.

Email and messaging

- Any message you send from our Council email system (or other messaging system) identifies the Council as the sender. Emails, texts and other electronic messages are therefore formal communications from the Council and should be treated as such. You must make sure that any information you send is appropriate and does not include any personal comments that may conflict with our policies or bring us into disrepute.
- You must follow the email guidelines.

Mobile devices

- You must take care with the security of any of our ICT resources, especially mobile devices. Do not leave equipment such as laptops and smart phones unattended in a vehicle or elsewhere.
- You must ensure that all mobiles devices are encrypted.
- You must not store information about citizens, customers or service users on a personal mobile phone or other device.
- If you have cause to contact a colleague's personal mobile phone or home phone but have to leave a message, this should be limited to basic information such as "please call me back". If someone else has left a message on your personal voicemail and this contains sensitive information, you should delete the message once you have listened to it.
- You must exercise caution when using a mobile phone in a public place in order to protect Council and service user information, and yourself.

You must **not** use our ICT resources as follows:

- For illegal activities, including defamation and fraud
- To run personal or private software or apps – there is a risk of viruses/malware to the Council network
- For any purpose that would breach our Information Security Guidelines, our Data Protection Guidelines, our Dignity at Work Policy or our Code of Conduct for Members and Officers.
- To install software or tools which undermine or bypass our security systems and policies. This includes any software that would:
    - Identify passwords for files and accounts
    - Secretly record keyboard input
    - Hide the user's identity
    - Intercept traffic transmitted across the network
    - Provide remote access to the Council's network

The above list of examples is not exhaustive.

If you are not sure whether your use of ICT resources is appropriate, please speak to your line manager.

7. Monitoring of the use of our ICT resources

By using our ICT resources, you accept that your usage may be monitored. Monitoring helps to maintain the efficiency and integrity of our ICT systems. Your use of ICT resources may also be investigated and/or monitored in the event of any investigation into alleged misuse of ICT resources.

8. Breaches of this policy or other misuse of ICT resources

Action will be taken against any individual who breaches this policy, or misuses our ICT resources. The action taken will be appropriate to the circumstances and may include disciplinary action up to, and including, dismissal. We may withdraw your permission for personal use of ICT resources if you have been found to breach this policy.

Breaches of this policy may be reported to the police and/or other professional bodies where appropriate.

If you are aware of any breach of this policy, you should advise your manager or supervisor as soon as possible. Please also refer to the Information Security Incident Reporting Procedure.

9. Employee benefits and resources

We recognise there are benefits to individuals from this policy, which includes the personal use of ICT resources as set out in section 5:

- Responsible and productive use of our ICT resources can enhance your skills and awareness.
- Personal use of ICT resources can help balance your work, lifelong learning and personal life.
- Personal use of ICT resources is an opportunity to provide a benefit to you at no additional cost to us.

You must complete a mandatory information security course each year if you use our ICT resources. The course reminds you of your responsibilities when using our equipment and how to handle and protect the information you use at work.

10. Other relevant policies

For more information, please read our:

- Information Security Policy
- Information Security Guidelines
- Guidelines on personal use of social media (attached)
- Email guidelines (attached)
- Data Protection and Confidentiality Guidelines
- Information Security Incident Reporting Procedure
- Data Security Incident & Breach Management Procedure
- Code of conduct for employee and members
- Dignity at work policy
- Mobile Flexible Working guidance

Version	Purpose/change	Author	Date
0.1	First draft based on Glasgow	Wendy Barber	28.2.18
0.2	Second draft after discussion with Ian Rennie	Wendy Barber	16.3.18
0.3		Ian Rennie	
0.4	Reviewed at meeting Wendy Barber/Ian Rennie	Wendy Barber	21.6.18
0.5	Updated with changes from FC	Ian Rennie	26.11.18
0.6	Final	Wendy Barber/Ian Rennie	23.1.19
0.7	Minor change to replace reference to Homeworking Policy to Mobile Flexible Working guidance	Wendy Barber	2.4.19
0.8	Format changes	Fiona Campbell	16.4.19