Technology and communication services governance policy

Published May 2025

Introduction

Information is critical in enabling us to deliver our services. ICT governance is about ensuring that all the information we encounter – whether about people or the organisation – is handled properly throughout its life cycle. All information must be collected, stored, used, shared and disposed of appropriately and securely by following legal requirements and best practice.

Sometimes responsibilities are not set by the organisation but are required by external bodies. These include the Care Inspectorate, the Scottish Housing Regulator (SHR) and the Scottish Social Services Council (SSSC). The SHR Code and the SSSC Code of Practice apply to all aspects of this policy. Additionally, we must meet the requirements of the Cyber Essentials scheme run by the National Cyber Security Centre.

We are subject to The Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation), as well as the Freedom of Information (Scotland) Act 2002.

Purpose

This policy defines our shared responsibilities in the use of any device, technology service or communications service used in support of our work.

This policy exists to protect those who receive support or housing from us, those who work or volunteer with us, visitors, contractors and lastly the organisation itself. All members of staff, as defined in our Staff/Applicant Privacy Notice, are obliged to familiarise themselves with this policy and refer to it on an ongoing basis to ensure that its terms are implemented and complied with.

A summary of responsibilities for all staff is provided, but we strongly encourage everyone to read the complete policy for the fullest understanding or if you are looking for greater detail about any specific area.

Breach of Policy

Employees should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, which would include but are not limited to activity causing serious damage to the organisation, may constitute gross misconduct and lead to dismissal.

Summary of responsibilities for all staff

For the fullest understanding, the main policy document must be read.

Security	• Access to data, even if held on paper, must be restricted to those who need this access. • Don't copy data belonging to Key to removable, storage such as USB drives. • Everyone gets the minimum access to network services, software and data needed to do their regular, daily tasks. • Exercise good judgement when using the web. • You must not view non-work-related web content. • Keep your password confidential and do not share it. • All work accounts must have multi-factor authentication enabled. • Only equipment provided by Key can be connected to wired or corporate Wi-Fi networks. • Use public Wi-Fi networks only for accessing virtual desktop services.
Devices and services	• Lock your devices when unattended. • Don't store device passwords or PINs where others can access them. • ICT ensures applications and third-party services are securely configured and managed. • If we provide you with a device, you must bring it and its charger to work. • Connect work devices to Wi-Fi in Key offices and when at home. • Report damaged or lost devices to ICT immediately. • Use only Microsoft 365 apps for messaging and collaboration. • Use Key email services only for business purposes. • Anything sent or received on Key devices/services is not private.
Procurement	• ICT handle all technology and communication purchases. • Pay-as-you-go mobiles are not allowed.
Data protection	• You cannot keep personal data for longer than it's needed. • Individuals can request data erasure when it's no longer needed. • Key must be able to justify how long personal data is kept. • You must not print outside of Key offices and worker bases.
Data handling and retention	• Store files in the appropriate folders within Microsoft 365 and VDI. • Don't copy files to personal devices or cloud storage. • Data retention periods are detailed in the data retention policy.
Bring your own device (BYOD)	• Use personal devices only when there is no other alternative. • Protect personal smartphones or tablets with a 6-digit PIN and regular security updates. • Use Microsoft 365 mobile apps for work and remove accounts when you leave us. • Use personal computers only for virtual desktop service. • Personal computers must have an account used only by you and an active anti-virus/malware subscription. • Don't connect personal devices to wired or Wi-Fi networks in the homes of people we support. • Don't connect personal devices to office networks by cable.

Security

The organisation implements many different methods to secure our data. These include physical measures and third-party services. Below is a summary of these measures. Users must take no action to circumvent these security controls.

Policy acceptance	During induction, new colleagues will be given a copy of this policy document and will be required to indicate their acceptance of its provisions.
Physical access to servers	Physical access to server rooms controlled by the organisation is restricted to members of the ICT and Business Continuity teams. Contractors and other persons can only access server rooms under the supervision of ICT staff.
Physical media	Access to data held on physical media, including paper, must be restricted to only those who require this access. Users must take all reasonable effort to protect this media and to ensure that we satisfy the provisions of the Data Protection Act 2018. Data belonging to the organisation must never be copied to any type of removable, portable storage such as USB flash drives. Where we operate CCTV services, the police will provide their own storage devices as necessary.
Logical access control	This is a security process that manages access to resources such as computers, networks, and data. It ensures only authorised users can access specific environments, protecting sensitive information from unauthorised access, tampering, or theft. It requires the validation of an individual's identity through some mechanism, such as a password, PIN, card, biometric, or other token. We provide logical access using the principle of “least privilege.” This ensures that users, and systems have the absolute minimum access required to perform their daily tasks, thereby reducing the potential for and impact of security breaches.
Use of the web	Given the nature of the whole life support we provide, the organisation does not utilise website blocking or content management and control software. However, end users are expected to exercise good judgement when using the web. You must not view content that is unrelated to your work with us. Nor should you view content likely to offend, considered obscene or that may be illegal. You will be responsible for all content viewed using your account.

We do take measures to protect ourselves. Our malware protection software features time of click URL protection. This blocks links to known malicious websites. If you are at all suspicious of any website, you should contact the ICT Support Team right away.

Identity management

Every person will have a unique user identity, which must never be shared. This identity links the user to their actions and makes them responsible for these actions. Records of user access may be used to provide evidence for investigations.

All users shall keep their passwords confidential, and these must not be shared with anyone. If a user suspects their account password is known to others, they must immediately change it.

All user accounts must have multi-factor authentication enabled. Users should have a least 2 methods registered.

If you need to store a copy of your password, this must be on a non-work provided device that no one else can access. Your username should not be stored on the same device.

The use of group or shared identities is permitted under only exceptional circumstances. These must be documented, and risk assessed ahead of time. They should also be subject to regular review.

Network security

ICT implement measures to separate servers, systems and users to limit the impact of any attack on our networks. These measures are detailed in the ICT Handbook along with the routing controls implemented to support this plan.

Only equipment purchased and provided by the organisation can be physically connected to Ethernet networks or wirelessly connected to corporate Wi-Fi networks. Whenever possible, ICT will provide guest Wi-Fi networks in the organisation's offices and bases. This is for business purposes only and there are limitations to where we can provide this.

Public Wi-Fi

Devices provided by the organisation, and personal devices used to access data belonging to us must only be connected to public Wi-Fi networks to access our virtual desktop service.

Public Wi-Fi includes, but is not limited to, those in retail establishments, transport services and other public venues. The security of such networks cannot be assessed; therefore, no other use is permissible.

Operating Systems	No standard user will be provided with administrative access to any device. Users must take no action to circumvent security controls. Devices issued by the organisation will be enrolled in a device management system whenever possible. All users must lock their device whenever they leave it. When a device is protected by a password or PIN these must never be attached to or stored in a way that allows others to access them.
System configuration	All default accounts provided with operating systems shall be disabled following system installation. All standard users must confirm they are an authorised user at log-on. All user workstations shall be configured to lock automatically after a period of inactivity to reduce the risk of unauthorised access. When a user account is no longer required, the account will be immediately disabled.
Application security	ICT teams shall ensure that applications utilised by us are securely configured and managed. They will further ensure that all applications are captured within the ICT inventory. This shall be used to manage application configuration, patches and updates. Vendor issued patches and updates will be installed as soon as is practicable. Virtual desktops and end user devices shall be configured to prevent the download and installation of unauthorised applications.
Anti-virus and malware protection	ICT teams shall ensure that effective anti-virus and anti-malware services are implemented. They will further ensure that: • Software is kept up to date. • Real time scanning is enabled. • Tamper protection is enabled to prevent malware from altering or disabling protection. Users must not: • Accept or connect removable media from colleagues or external persons.

Secure configuration	Access to systems and data is based on the principle of least privilege. Baseline security configurations shall be developed in conjunction with security best practices from hardware and software vendors to ensure a consistent build status for all client and server systems. Protective monitoring shall be in place to detect any attempt to modify the configuration of client and server systems. All client systems shall be configured to start into a secure state. It should not be possible to modify the startup configuration.
Device encryption	Whenever possible end user devices shall be protected by a full disk encryption solution approved to protect the identified security classification. If full disk encryption solution has not or cannot be configured on the device, then the risks to the information shall be assessed and either: • An alternative encryption solution shall be utilised for which the risks have been accepted by ICT services. • or the risks shall be qualified and accepted by both ICT staff and operational managers.
Security updates and patching	ICT staff shall ensure that infrastructure and associated components comply with baseline security configurations. ICT staff will ensure that server, commercial off-the-shelf applications and in house owned or managed apps are patched and updated as quickly as possible after release. End users must ensure that updates to applications and operating systems on devices issued to them are applied whenever they become available.

Devices and services

Business devices

When we provide you with a device or service, it must be:

- Used for work purposes only.
- Used only by you, unless specified as a shared device.
- Used in a manner that is ethical, legal and upholds our values.

If a device is portable or battery operated you must have the device and its charger with you, ready to use whenever you attend work.

If the device supports Wi-Fi, you should ensure that you are connected to Wi-Fi in Key's offices and when using the device at home.

Where we provide you with a device it will be managed by us. This is to enable us to keep it up to date, apply security updates and monitor its use. We will endeavour to do this "behind the scenes" as much as we can.

If updates require that you restart your device, you should do this as soon as possible after the updates have installed. If you do not do this our management software will force a restart. This may not be at a time that is convenient for you.

If a device we have provided to you is damaged or lost, you must report this to the ICT Support Team without delay.

User accounts

Everyone who works with us is provided with a Microsoft 365 account. This account provides access to Microsoft's online services, as well as apps on smartphones and other devices.

Whenever we shop or bank online, we are asked to verify our identity. This is often in the form of a username and password. Nowadays, we are often asked for additional information. This may be answering a security question, using a code shared by text, a phone call or by using an app or device. This is called multi-factor authentication.

When accessing our services, we will ask for 2 ways of verifying who you are. This is something we must do to preserve our Cyber Essentials accreditation. We are contractually obliged to maintain our Cyber Essentials status.

Your Microsoft 365 account can store several additional ways in which to verify your identity. We encourage you to set up at least 2 additional methods. The primary method should be the Microsoft Authenticator app.

Online services	The organisation uses Microsoft 365 and a small number of approved services such as Canva. Microsoft 365 is a collection of online apps and services. Included are apps for messaging, meeting, and collaborating, as well as email and web versions of the core Office apps. Users can access these apps and services on a variety of devices wherever they are. Requests to use other online services should be made to the ICT Support Team. If you request a service we have not vetted for others, it will be subject to a feature and security review. If a requested service replicates something available in Microsoft 365, we will direct you towards the feature we already support.
Apps on business devices	Smartphones, tablets, and computers are provided with a standard set of apps that enable the use of Microsoft 365, virtual desktop infrastructure (VDI) and other approved business applications. Additional apps may be installed on smartphones and tablets by contacting the ICT Support Team. If you request an app we have not vetted for others, it will be subject to a security review. For example, apps often store data on their servers. The Data Protection Act 2018 requires organisations to confirm data is stored only within the UK or the EU. Apps that do not store data within the UK or the EU cannot be used.
Messaging apps	Collaborating with teammates must be restricted to the apps we provide. You must not use other apps, even on personal devices, to message or share information that relates to the organisation's business. Microsoft Teams is a workspace for real-time collaboration and communication, having meetings, and for sharing files and apps. It is available to everyone working with us. This app is our preferred tool for accessing the information you need to do your work. SMS (standard text messages) must always be a method of last resort and must never be used for time-sensitive messaging.

Email	Email is available to everyone, and it is to be solely used for business purposes. Email is the most common route for cyber-attacks, and we are working to reduce its use. You should open every email with caution and suspicion. Your email address is effectively an electronic representation of our letterhead. You must not put anything in an email that you would not put in a paper-based memo or letter. If your email includes sensitive or personally identifiable information (in its text or as an attachment) it must be encrypted before sending. Support workers and relief register workers must not routinely email persons outside the organisation. Exceptions to this restriction must be agreed with your Support and Development Manager. Concessions should be locally documented and subject to regular review and monitoring.
Monitoring of use	Microsoft 365 allows us to gather a range of information about how both devices and user accounts are used. Any communication sent or received via Microsoft 365 is the property of the organisation and can never be considered private for the purposes of monitoring or auditing. Monitoring may be carried out by ICT staff or senior and line managers. Senior and line managers can request time limited access to another person's account via the ICT Support Team. The access will be logged detailing the purpose of the request.

Procurement

Purchasing related to technology or communications (both hardware and services) is done centrally by the ICT teams. The teams have access to national frameworks that bring reduced costs and centralised management features.

Fixed landline, mobile phone and cloud telephony services are secured through these centrally negotiated contracts.

Only in exceptional circumstances, and in prior agreement with ICT staff, can landline and mobile phone contracts exclusive of the provisions of the centrally negotiated contract be used.

Pay as you go mobile phone connections are not permitted as they do not meet the financial audit requirements for the organisation.

Data protection

Data Protection legislation requires we retain personal data no longer than is necessary for the purpose the information was obtained for. Ensuring personal data is disposed of when no longer needed will reduce the risk that it will become inaccurate, out of date or irrelevant.

- We must not keep personal data for longer than we need it.
- Individuals have a right to erasure when we no longer need their data.
- We must periodically review the data we hold, and either erase it or anonymise it.
- We must be able to justify how long we keep personal data.

If data is being retained in perpetuity for a special lawful purpose, it must be held separately from all other data and only ever be accessed for the stated special lawful purpose.

The organisation has a separate policy addressing data protection needs. For a fuller understanding you should also read this policy.

Data handling and retention

We all have a professional responsibility to keep accurate files about our work and to store these in the right places. Files can be anything written, photographed, typed, copied or recorded in the course of our work. These include notes, reports, emails, letters, images, and audio-visual recordings. All data generated during your work with belongs to Key.

The way information is recorded, stored, and shared is crucial.

Files should be created using the devices provided by the organisation, using centrally published templates where appropriate, and stored in the appropriate files or folders within our Microsoft 365 and VDI environments.

All data must be compliant with our separate data retention policy. Therefore, files must never be copied to or held on personal devices or held within personal cloud storage services, including personal Microsoft 365 subscriptions.

Protecting our access to data

Data held in shared network drives, in emails, in Teams and in SharePoint are backed up to servers based in 2 different server rooms in Glasgow. A third copy is also kept on removable media. These backups are retained for 13 weeks and allow accidentally edited or deleted files to be restored.

Our backup servers do not have access to files on local drives, or to your OneDrive for Business folders. Therefore, data required by others in the organisation must never be stored in these locations.

Data retention

Acts of Parliament and regulatory requirements detail when we may retain personal data, when we must destroy it and when we must provide data that is in the public interest.

The length of time we will keep data varies according to the type of data we are using. A full schedule of data types and retention periods is contained in a separate Data Retention Policy.

Bring your own device (BYOD)

When we have provided you with a work device, you must use this device whenever you attend work. Personal devices can be used for work purposes only when there is no other alternative.

Using personal devices for work-related purposes creates several issues that need to be addressed, particularly around information security. Here we set out the responsibilities of staff members taking advantage of BYOD, and the circumstances in which we may monitor use of or restrict access to our data and services.

Using your own smartphone or tablet

- The operating system must be supported by regular security updates. If your operating system does not meet this requirement, you will not be able to access apps and data belonging to the organisation.
- It must only be used by you. Shared devices do not meet the requirements of the Data Protection Act.
- It must be protected by a minimum of a six-digit PIN. If your device supports biometric identity features, such as fingerprint or facial recognition, you should use these to enhance account protection.
- You must install the Microsoft 365 mobile apps – These approved apps are published by Microsoft to either the Apple AppStore or Google Play Store. At a minimum the Authenticator, Outlook and Teams apps will be used to access data belonging to us.

Using your own computer

Personal computers can only be used to access our virtual desktop service. Data belonging to Key must never be copied to or held on personal devices.

- You have responsibility for the security of your own device. You should be familiar with the operating system and the security tools it may contain. The operating system must be supported by regular security updates, and you must undertake to install these updates whenever they are released.

- Your device must have an active subscription to anti-virus and anti-malware applications. In some cases, for example Microsoft Windows, the built-in protection will be enough to satisfy this requirement.
- Your device must have a password protected account that can only be accessed by you. If your computer supports biometric identity features, such as fingerprint or facial recognition, you should use these to enhance account protection.

In the workplace

Where available, you may connect your personal device to guest Wi-Fi networks provided by the organisation when you are using it for work purposes. *Guest Wi-Fi is not available at all locations.*

Personally owned devices must never be connected to Ethernet or Wi-Fi networks used in the homes of people we provide services to.

Personal devices with Ethernet ports must never be connected to physical networks within any office or worker base.

You must not store personal documents or other data on servers or storage belonging to the organisation or to people who receive our services. You must not use printers or copiers belonging to the organisation for personal purposes.

At home

You must not print any information belonging to the organisation at home. This is to ensure our compliance with the Data Protection Act 2018 and our obligations under the Cyber Essentials scheme.

Costs

You must pay for your own device costs under this policy including, but not limited to, voice and data usage charges and any purchase and repair costs. You are responsible for all costs associated with the device and understand that your business usage of the device may increase your voice and data costs.

Technical support

The ICT Support Team will provide limited technical support to help you access our systems.

When you leave us

All data and communications are the property of the organisation. Therefore, on or before your last day of work for the organisation, all accounts and apps provided by us must be removed from your device. If this cannot be automated, you must provide all necessary co-operation and assistance to the ICT Support Team to facilitate the removal.