Key and Community Lifestyles

Information and Communication Technologies Policy

Information and Communication Technologies Policy

This policy should be read in conjunction with Key's separate policies on data protection and procurement.

Introduction

Information and communication technologies (ICT) are integral to the work undertaken by Key. Key is committed to using these technologies in a secure, efficient and legitimate manner. It fully supports compliance with the General Data Protection Regulation, and other legislation relating to the use of information and communication technologies.

The purpose of this policy is to ensure that the organisations technologies are used in a manner which is ethical, legal and appropriate to Key's values, and not used to the detriment of others. These technologies include, but are not limited to, computers, email, the Internet and Internet services, social media, messaging services, mobile phones, and fixed landlines.

The policy sets out the conditions of use of these technologies and provides a set of procedures that ensure responsible use of equipment provided by Key. The policy also exists to minimise the risks these technologies bring to Key, the people we support, our employees and our information systems.

This policy is relevant to all ICT equipment irrespective of the use or location, and applies to:

- All Key employees and volunteers.
- Employees and agents of other organisations who directly or indirectly support or use Key's communication infrastructure.

The following are straightforward conditions and procedures which must be observed at all times.

Equipment and Services

Key's procurement of products and services related to ICT are subject to a separate procurement policy as well as external regulation. No purchasing or contracting is permitted without the agreement of ICT staff.

ICT staff makes use of a number of nationally agreed purchasing frameworks to secure best value.

Fixed landline and mobile phone services are secured through one such centrally negotiated contract. 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.

Data Protection

You must treat confidential information in accordance with Key's separate policy relating to Data Protection. The General Data Protection Regulation and other UK-based legislation contain provisions relating to the retention and disclosure of data concerning individuals. This includes information held electronically as well as on paper.

The definition of an individual includes, but is not limited to, the people supported by Key, people employed by Key and employees and agents of other organisations Key may work in partnership with:

- Work relating to Key and its activities must never be stored on computers or cloud-based storage systems owned by or subscribed to by employees.
- Only commit information relating to Key, its employees or the people it supports to paper when it is absolutely necessary.
- Information must only be shared with external parties when an explicit data sharing agreement permits this.
- If you believe personally identifiable information has been misplaced or lost, you must report this immediately to Key's Data Protection Officer.

Use of Computers

ICT equipment is provided for work purposes. This includes its use in giving direct support to the people who use Key's services. ICT equipment must not be used for personal or recreational use or private gain.

If you believe that ICT equipment has been improperly used you must report this immediately to your line manager or to ICT staff.

Settings and security:

- You must not alter the settings of your computer or the network. Installations are generally standardised to aid support and maintenance.
- You must not attempt to gain access to parts of the system or network to which you do not normally have access rights.

Automatic Updates:

- Important security and software updates download automatically on computers connected to the Internet.
- Updates should be installed as early as possible after they have been downloaded.

Passwords:

- Access to all systems is controlled by a logon user name and password. User passwords are renewed on a schedule set by ICT staff.
- This password should never be disclosed to another person.
- Compromised passwords should be reported to ICT staff immediately.
- Passwords must never be written down or displayed to permit others to see it.
- When leaving a computer unattended, you should always log off or shut down the computer.

Where to save your work:

- All work relating to Key must be stored in the folders or network drive set up by and agreed with ICT staff.
- This will ensure that the data will be properly backed up.

Folder structures:

- Folder structures must not be altered, extended or put to alternative use by users.
- If a structure does not meet the needs of the organisation a review should be sought with ICT staff.

Using removable media/drives:

- Information relating to individuals must never be saved to removable media.
- Key's virtual desktop environment provides access to information from any location with an Internet connection.
- Where information not related to an individual is committed to removable storage, the media/drives must be owned by Key and use data encryption software to prevent unauthorised access.
- The removable media/drive must never be the sole or primary location for this data.

Relocation of equipment & services:

- Once installed no computer, telecoms or electronic office equipment should be moved without first discussing this with ICT staff.
- This is to ensure the continuing availability of Internet and network services as well as meeting Key's asset management requirements.

Virus protection :

- Antivirus software is installed on all computers and is set up to operate automatically.
- The software is configured to update itself each day.

Backups:

- Backup of data is done automatically.
- This backup data is held on servers within either Key's main administrative office in Glasgow or its designated business continuity site.
- The backups are, in turn, archived for up to 12 weeks.

Computers owned by the people Key support:

- Employees can use computers belonging to people supported by Key only in the following circumstances;
- to provide direct support to the individual
- to access Key's virtual desktop environment to complete administrative tasks relating directly to that person and with their prior, informed consent

Computers owned by employees:

- Employees should not use personal or family owned computers, except as a means to access Key's virtual desktop environment.
- Administrative tasks must only be carried out on physical or virtual computers belonging to Key.
- Computers owned by employees must never be brought in to the workplace, nor connected to wireless or wired networks belonging to Key or the people Key support.

Use of Telecoms:

- Fixed landline and mobile phone services are provided in liaison with Key's ICT staff.
- This allows for compliance with centrally negotiated contracts and Key's policies on procurement.
- Changes to existing services or securing new services should be done via Key's ICT staff.

Fixed line and mobile phone handsets:

- Key's ICT staff will supply fixed line and mobile phone handsets appropriate to business needs and contract provisions.
- If a handset is damaged, it should be reported to ICT staff straight away.
- Employees must never transfer a SIM to another handset except upon the instruction of ICT staff.
- Users must not change or remove any PIN set on the device by ICT staff.

Pay As You Go (PAYG) mobile contracts:

- This type of mobile contract does not comply with Key's financial audit requirements and must never be used.

Smart phones and Internet enabled devices owned by employees:

- Devices owned by employees may be configured by ICT staff to connect to wireless networks operated by Key to facilitate email services when a business convenience has been demonstrated.
- Where Key's email is accessed in this manner, users must agree to use an access PIN on their device and permit Key to remote wipe the device should it become compromised.
- Internet enabled devices owned by employees should never be connected to wireless or wired networks belonging to the people Key support.

Smart phones and Internet enabled devices owned by people Key support:

- Devices owned by people we provide support to should never be connected to wireless or wired networks operated by Key.
- The only exception to this rule is within short stay services where additionally an individual undertaking has been entered in to as part of the short stay contract.

Use of the Internet, Email and Social Media

- Key encourages use of the Internet, email and social media for activities relevant to the aims and objectives of the organisation, including the direct support of the people we provide support to.
- Employees are expected to exercise responsible and appropriate behaviour when sending email, whether externally or internally, or when using the Internet, including social media websites and applications.
- Personal use of the Internet, email or social media is not permitted.
- You must discourage the sending of email to your account that does not relate to the business of Key.
- You must not use the Internet, email or social media to view, store or distribute any material that may be construed as obscene, offensive or of a discriminatory or harassing nature in any way.
- Should there be evidence of any abuse of this nature disciplinary action will be taken.
- You are responsible for all use of the Internet, email and social media carried out under your username and password.
- Masquerading as/or misrepresenting another user is prohibited.

The Internet

Much valuable information is available from the Web. Many organisations have a presence on the Web to provide up-to-date information and advice. Internet shopping and online services are commonplace. The Web also contains unpleasant, inaccurate and illegal media. For this reason it is important that employees using the Internet in the course of their work abide by the principles of this policy.

Access to the Internet:

- Everyone has access to the Internet for business purposes.
- Internet connections must only be set up by ICT staff.

Internet Services:

- You must not subscribe to any Internet services (including, but not limited to file sharing or third party messaging services) without the agreement of ICT staff.

Using copyrighted materials obtained from the Internet:

- Information found on the Internet is subject to the copyright laws covering printed publications and audio releases.
- Only content that is stated as being free of copyright or royalty restrictions or is released through the Creative Commons scheme should be used within presentations, broadcasts or publications issued by Key.
- Confirmation of the legal copyright status should be stored along with the electronic files.
- If required by the Creative Commons license, a public attribution of copyright should also be included within the presentation, broadcast or publication.

Email

Access to email:

- All employees have access to email.
- Key's email address should only be used by employees of Key for business purposes.

Email contents:

- All emails are effectively an electronic representation of Key's letterhead.
- You should not put anything in an email that you would not put in a memo or letter.

The following procedures are recommended practice:
Consider whether email is the best way to send a message;

- Messages may not be secure.
- Messages may be produced as proof that you said something.
- Messages may be held to be legally binding.
- Messages may be subject to tampering after delivery or sending.

Apply the same principles you would use with a printed memo:

- Content should be clear and not open to misinterpretation.
- Use plain English.
- Include a meaningful and logical subject line.
- If the recipient is not expecting the email and does not recognise the subject of the data they may delete it.

- Always telephone the recipient if they are not expecting something unusual.
- Include your position and contact details the first time you correspond.
- Only copy to those who need a copy.
- If you are transmitting sensitive data, send it in a password protected document or folder. This password must be shared via a means other than email.
- You must not send, forward or redirect any obscene or defamatory emails, or emails containing foul language, bullying, harassment or discrimination of any kind.
- You must not send emails that could be construed as sexual harassment.

Access to other people's email:
- You must not attempt to gain access to email messages of other employees, except where this is provided to you for monitoring purposes.

Signature and disclaimer:
- All email messages carry the organisation's centrally managed signature.
- The content of this signature is populated by Active Directory fields.
- All external email messages carry the organisation's disclaimer which you cannot alter or delete.

Written record:
- Any important email exchange should be filed in an appropriate manner to maintain a record of this correspondence.

Social Media

If you are required to use social media as part of your work with Key, you must do so in line with the requirements of the Code of Conduct for RSL Staff Members. The same professional expectations and guidelines for interacting with people in the real world apply to online communication and information sharing and you must always be a positive ambassador for Key and our work.

Information posted via websites and social media applications is classed as public and not private. You must not disclose any private or confidential information relating to Key, the people we support, or our suppliers, board members or other employees. This applies whether you are posting under your own name or using a pseudonym.

Employees must not access social networking sites for personal use during work time. Posting information or comments related to your work with Key (even in your own time and using equipment owned by you) may be viewed as misconduct and be in breach of Key's policies.

Monitoring of Use

Computers, email, the Internet, mobile phones and fixed landlines are installed expressly for the purpose of supporting the work of Key. In most instances, their use is automatically recorded. Key will routinely monitor the use of the communication methods covered by this policy statement.

This may be done by, but not limited to, accessing billing information, computer logs and mailbox contents. Among the reasons for this monitor are:

- Detecting viruses.
- Prevention of unauthorised access to Key's systems.
- Inappropriate use of the Internet or email as defined by this policy.
- Detecting unusual trends in use of Internet or email services.
- All email messages sent or received via Key's email address are the property of Key and can never be considered private for the purpose of monitoring/auditing.
- Monitoring of email messages may be carried out by ICT staff or senior and line managers.

Breaches of Policy

Employees must conduct themselves in a trustworthy and appropriate manner in accordance with the spirit of this policy statement so as not to discredit or harm Key or its staff.

Failure to adhere to this policy can result in disciplinary action, the exact nature of which will depend on the breach.

The use of ICT systems for any criminal activity or if used in an obscene or offensive way will be viewed as gross misconduct and action will include the possibility of dismissal from the organisation.

Review of Policy

This Policy will be reviewed annually to take account of both legal and technological developments and the changing needs of Key.