Kent County Council
ICT User Standards
Issued By Human Resources

Reviewed April 2020

Contents:

1. Introduction

Kent County Council (KCC) is responsible for ensuring the confidentiality, integrity, and availability of the information that it processes and stores in its Information Communication and Technology (ICT) systems in order to provide its services and facilities. KCC has, therefore, an obligation to provide appropriate protection against threats which could adversely affect the security, integrity and availability of its ICT systems and/or their associated data.

This Standard supports KCC's 'ICT Acceptable Use Policy' which gives KCC's expections of the behaviour, attitude and work ethics adopted by persons in their use of its ICT equipment and systems to carry out work for and on behalf of KCC.

2. Objectives

The objective of this Standard is to state, in a more prescriptive manner, how KCC's ICT equipment and systems can and cannot be used.

This Standard is designed to ensure the security, integrity and availability of KCC's ICT systems and equipment and to protect the rights of their users.

3. Scope

'ICT' for the purposes of this Standard is any network, electronic device, system or service that can process, store and/or transmit information electronically.

This Standard covers all KCC employees, members, partner agencies, agency staff, contractors and volunteers who use ICT in the course of their duties for and on behalf of KCC. If you use ICT to carry out work for and on behalf of KCC then this Standard applies to you.

KCC's other relevant policies, standards, processes and procedures, such as those listed in section '7. Supporting and Reference Documents', should also be read and understood.

4. Risks

Using ICT is often essential to do KCC business. However, it and its users have the potential to expose KCC to risks of criminal prosecution or civil litigation resulting from the following:

- defamation
- discrimination: whether on the grounds of gender, gender identity, race, disability, sexual orientation, religion and belief, age or any other protected characteristic
- breach of legislation, including but not limited to: data protection, electronic communications, computer misuse, obscene publications and civil contingency
- breach of copyright
- breach of contract

- breach of the duty of confidentiality.
- Additionally, the downloading, installation and use of unauthorised software could expose KCC's ICT infrastructure to malicious code (including viruses and Ransomware) that has serious effects on the security, integrity and availability of KCC's business system applications and, thereby, the business-critical services that they support. It could also result in litigation for breach of software license arrangements.

5. Standard

KCC provides you with ICT devices, systems and services and/or the ability to access its network and systems to help you do your job.

KCC reserves the right to withdraw ICT devices, systems or services, if they are misused or abused.

5.1 ICT access and use

- You must:
  - comply with the KCC's Information Security Policy, ICT Acceptable Use Policy, User Identification and Authentication Policy and Remote Working Policy.
- You must not:
  - disclose your personal log-in credentials (i.e. passwords, passcodes or PINs) to anyone else (including ICT support or administration personnel). Refer to KCC's User Identification and Authentication Policy.
  - attempt to disable, bypass or circumvent the security and integrity controls and mechanisms applied to your KCC-provided electronic device(s)
  - leave a work station unlocked
  - install or download software. Any requirement for software (and devices that require software/apps) must be referred to the ICT Service Desk beforehand so that the security, integrity, compatibility and software licensing requirement aspects of the request can be appropriately risk assessed.
  - store personal client data unless the storage is covered by KCC's Data Protection registration under the UK's Data Protection Act (2018) or the EU's General Data Protection Regulation (2016)
  - upload KCC data to cloud storage systems other than KCC's corporate cloud storage solution without consulting your line manager, providing a justifiable business case and carrying out a formal Information Risk Assessment beforehand. Refer to KCC's 'Safe Use of Removeable and Online Storage Policy' for more details.
  - store electronic documents on KCC equipment that are personal to you and not related to work activity (e.g. photographs, video files/MP3, music files)

- enable KCC property to be stolen by not applying reasonable measures to secure it when away from KCC premises. Refer to KCC's 'Information Security Policy' and 'Using IT for Remote Mobile Working Policy' for more information.
- engage in criminal activity such as denial of service attacks, fraud or spoofing (e.g. masquerading as another system, web-site person) or radicalisation.

5.2 Email, Instant Message and Collaboration tools and services

- You must:
  - adopt a responsible approach to the content of emails, instant messages (such as Microsoft's 'Skype) and collaborative audio/video sessions (such as Microsoft's 'Teams') bearing in mind that these often need to be as formal as any other form of correspondence such as a letter or official meeting.
  - use KCC's secure e-mail service when the contents of the e-mail is considered to be personally, politically or commercially sensitive. Please see KCC's 'Secure Email Policy' for more details.
  - be aware that emails, instant messages and transcripts of collaboration audio/video sessions may be disclosable in any legal action against KCC or in response to a Freedom of Information request and that emails which have been deleted by a user or from the network may be recovered subject to system capability.
  - remember email and instant messaging correspondence is not private because these can be easily copied, forwarded or archived without the original sender's knowledge. When drafting such correspondence you need to bear in mind that it may be read by a person other than the person you sent it to.
  - consider providing links to large documents when these are required by many internal or external recipients rather than sending each recipient a copy of the document as an attachment to an e-mail. KCC's SharePoint and/or Teams services can also be used as alternatives to sending large email attachments. Great care should, however, be taken with setting the 'Permissions' of and 'Links' to folders, sub-folders and files that are to be shared with others via SharePoint and/or collaboration tools/services such as Teams. Such Permissions can be set to: read-only; to edit; to download and/or; to forward on to others as is appropriate to the sensitivity of the information and the purposes and objectives of the correspondence. Care must also be taken to remove Permissions and Links when access to the folders/sub-folders/files is no longer required by the other parties. Similar care should be taken with the granting membership to 'Teams' sites – especially for 'Guest's'. Remember, all access to systems, information and Teams sites should be on a needs-only and least privilege basis. Please refer to the 'Information Governance for External Sharing' e-learning course on KCC's/Delta's training platform for more information and advice in setting up, removing and managing file permissions and Teams sites.

- keep hard copies of emails only where this is necessary for KCC records and manage electronic records properly (in accordance with KCC's Information Governance Policy; Information Governance Management Framework and; Information Security Policy)
- delete all personal emails and attachments when they have been read or sent.

- You must not:
  - open attachments to emails from unknown sources
  - send emails and/or instant messages that are abusive, malicious, discriminatory, defamatory about any person or organisation, or which contains illegal or offensive material or foul language
  - send or forward unsolicited bulk email messages, chain mail or "spam"
  - auto-forward messages received in your KCC account(s) to personal or other email accounts without consulting ICT's Service Desk first.

5.3 Internet

- You must:
  - Access the Internet only through the official service provided by KCC which monitors all activities and may block access to certain web-sites.
  - Remember that internet sites are in the public domain and you are accountable for any statements you make (including those relating to your employment with KCC or about the Council).

- You must not:
  - use WiFi provided in hotels, conference centres, Internet cafes, restaurants, coffee shops, railway stations, airports and other public places unless you have referred to KCC's 'Information Governance Policy', 'Information Security Policy' and 'Using IT for Remote Working Policy' and have personally risk assessed the situation.
  - use the Internet for illegal or criminal activity, for example but not limited to software and music piracy, terrorism, cyber-related attacks or the sale/purchase of illegal drugs
  - visit, view or download any non-job-related material from any Internet site containing illegal material (such as child pornography, obscene material or race/hate) or other inappropriate material. Examples of inappropriate material include but are not limited to: criminal skills; terrorism; cults; gambling; illegal drugs and; pornography
  - copy or modify copyright protected material downloaded from the Internet without obtaining authorisation from the copyright holder beforehand
  - enter into a contract and/or software licensing arrangement via the Internet without following KCC's procurement and authorisation procedures. A

contract/ software licensing arrangement entered into via the Internet is likely to be legally binding in the same way as any other contract

- use your KCC log-in credentials or KCC e-mail address as your account ID when registering with non-KCC work related Internet-based services
- use your personal e-mail address to access KCC work related Internet-based services or to send KCC work-related e-mails.
- You must not use KCC ICT user credentials to conduct personal financial transactions.

5.3 Social media

- You must:
  - use social media, if accessed using KCC's network, only if this is required as part of your job or work;
  - know and follow The Kent Code, ICT Acceptable Use Policy and Social Media Framework Guidance;
  - remember that all social media sites are in the public domain. You are accountable for any statements you make (including those relating to your employment with KCC or about the Council) whether or not you used KCC ICT equipment and resources to post them;
  - be responsible and professional and consider how the information you are publishing could be perceived;
  - use social media provided by KCC, such as Yammer and 'Your Voice', in a responsible way which includes not posting messages which are abusive, malicious, discriminatory, defamatory about any person or organisation, or which contain illegal or offensive material or foul language.
- You must not:
  - use your KCC email account for updates from Facebook or other personal social networking sites;
  - use your KCC credentials to subscribe to or to access a non-KCC business related bulletin board, newsgroup, social networking medium or any other similar Internet service.

5.4 Personal use

- The equipment and resources KCC provides are to be used to conduct KCC business. Limited personal use is allowable provided it: does not breach this policy, does not interfere with the delivery of your work; affect expected levels of your performance; is with your line manager's permission and; does not affect the performance of KCC's network and/or ICT infrastructure.
- You must
  - keep all personal email messages short

- ensure that all personal use takes place at times and in volumes of activity that does not interfere with your performance or affect the business use of the network
- ensure that the use of radio, media streaming, MP3, or iPods is appropriate to the working environment, is with your manager's agreement and does not cause interference to either the users or those around them. Be aware that the streaming of radio, music, video or podcast content is for personal use only and any sharing of these may be subject to copyright or broadcasting restrictions and/or legislation.

- You must not
  - spend excessive time: surfing the Internet for non work-related purposes or; on KCC Noticeboards
  - download and/or install on your KCC device(s) apps for downloading and/or streaming radio, music, video or podcast programmes.

5.5 Monitoring

When using KCC's network, ICT systems or equipment your expectation of privacy cannot be guaranteed as all use is monitored. If you want to ensure the privacy of any personal information you should use a personally-owned device or internal post and not KCC's email, instant messaging or collaboration systems and services.

KCC's ICT service provider, on behalf of KCC, undertakes regular monitoring of the use of its ICT systems and equipment for lawful reasons to protect the integrity and security of the systems and to investigate suspected unauthorised or inappropriate use.

Line managers also have a responsibility for monitoring the use of ICT and ensuring that persons within their remit are aware of their responsibilities particularly when accessing or inputting sensitive data (e.g. client systems, payroll).

Any monitoring will be carried out subject to the requirements of legislation including the EU's General Data Protection Regulation (2016), and, HMG's UK Data Protection Act (2018), Human Rights Act (1998), Regulation of Investigatory Powers Act (2000) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000).

KCC's intention is that any monitoring will be proportionate to the risks of harm to KCC's reputation or operational capability and the confidentiality and integrity of information it processes and stores. Your privacy as a user will be respected as much as possible. Monitoring is carried out in the same way regardless of whether the user is office based or working remotely.

Such monitoring identifies the physical location of the user. Access to KCC's network and ICT infrastructure provides links to central government's systems and online services that are otherwise restricted. Please be aware that access to certain central government systems, from outside the UK, is prohibited. Similarly, access to KCC's network and ICT infrastructure from certain countries and regions around the world may be considered to present unacceptable risks. As a result, attempts to log-in to KCC's network and ICT infrastructure from outside of the UK, may result in ICT

disabling the user's account. KCC devices cannot be used when outside of the UK on annual leave.

Network traffic and the performance of the network is monitored: KCC uses a firewall; an anti-virus/malware product; an intrusion detection system and; other software to do so, as follows:

- anti-virus/malware software monitors all communications but will only record and quarantine those which it identifies as containing a virus or other malicious code
- software monitors emails for the use of profanity and the file types of attachments. Emails to external parties containing profanity will be quarantined. Attachments of file types that are not on KCC's list of approved file types will not be delivered to the intended recipient. For a list of acceptable and unacceptable file types, search for 'Allowed Incoming and Outgoing File Attachments' within Cantium's ServiceNow portal's 'Knowledge Base' section.
- software is used to monitor the content of emails or the content of Internet sites visited. A user's account may be disabled when KCC reasonably suspects that such content may present a risk of compromise to the security and integrity of its ICT equipment and resources, or has received a complaint that a user is misusing the KCC's network and/or is not following the standards set out in this Standard
- software will prevent access to certain designated non work-related Internet sites. Access to a blocked site(s) can be allowed for specific business purposes subject to line management assessment of the business case, ICT's risk assessment for security vulnerabilities and threats and subsequent approval.

Access to users' Emails and Work Area. Your manager may, where necessary, request access to your email account and/or your work area if you are absent from work due to sickness, holiday or any other reason. If you plan to be away from work for any period of time you should make arrangements, in advance, for your line manager to access your emails or other files. Contact the ICT Service Desk for guidance.

6. Responsibilities and Policy Compliance

6.1 KCC

KCC's primary responsibility is to provide equipment that supports you in working effectively in your role, supporting the business and providing a service to the public. Support from the ICT service provider is available to ensure that the equipment you use is properly maintained and you are trained and supported in its use.

6.2 Managers, Supervisors and Team Leaders

Managers, Supervisors and Team Leaders are responsible for ensuring that:

- all personnel within their remit are aware of and have read and understood this Standard
- this Standard is adopted and followed

- this Standard and its associated Policy are incorporated within and/or translated into formally documented operational processes and procedures
- all personnel within their remit who are moving or changing roles or leaving KCC's employment have their access rights to KCC's systems and information amended accordingly.

6.3 Your responsibilities

As a user of KCC's ICT equipment and systems (including access to its network using devices not provided by KCC) you must comply with this Standard at all times.

By accessing and using KCC's ICT systems and services, you are deemed to have read, understood and agreed to adhere to this and other relevant policies and standards.

Your access to ICT is accountable to you through log-ins, user accounts and passwords which must not be shared.

You should report misuse of KCC's ICT systems to your line manager in the first instance or to a Directorate Contact Point (details of which can be found in KCC's Whistleblowing procedure).

If you suspect that the security and/or integrity of electronically stored information has been compromised – especially if the information is of a personal or sensitive nature – you should inform your line manager immediately and refer to KCC's Data Breach Policy.

6.3 Training and Awareness

All personnel should feel confident that they are aware of their personal responsibilities in respect of this Standard and are competent to carry out their duties. Information, advice and guidance can be found on: KCC's KNet; KCC's corporate e-learning and face-to-face training service provided via Delta and; Cantium Solutions 'Service Now' portal's 'Knowledge Base'.

6.4 Standard Compliance

KCC expects you to act responsibly and professionally at all times when using its ICT equipment and systems and to be accountable for your actions.

Participation in activities that brings KCC into disrepute or contravenes any of its policies or the law or negligent and/or deliberate misuse of ICT equipment or resources will result in disciplinary action and, in the most serious of cases, dismissal for 'gross misconduct'.

6.4.1 Gross Misconduct

The following are examples of gross misconduct when using KCC's ICT equipment, devices, systems and services. You are likely to lose your job if you are found to be misusing our equipment in any of these ways:

- sending or posting on internal and or external sites abusive, rude, illegal, discriminatory or defamatory messages or material

- sending bullying or harassing messages
- compiling or distributing chain letters either internally or externally
- sending and uploading restricted and/or confidential/sensitive information without authorisation
- excessive personal use of email or the Internet in work time
- the introduction of a virus or other malicious code onto the KCC system resulting from negligent or malicious behaviour
- misuse of email, the Internet, Social Media or the system generally which results in a legal claim being made against KCC
- accessing illegal material or pornography on the Internet
- unauthorised copying or modifying of copyright material or material protected by any other intellectual property rights
- unauthorised downloading of software or files
- unauthorised installation of software, including apps, that breach software licensing contracts/agreements
- use of the Internet for criminal activity
- hacking, or other breaches of the Computer Misuse Act 1990

7. Supporting and Reference Documents

- HMG's 'Data Protection Act (2018)
- EU's 'General Data Protection Regulation (2016)'
- KCC's 'Information Governance Policy'
- KCC's 'Information Governance' pages on KNet
- KCC's 'Information Management Manual'
- KCC's 'Information Security Policy'
- KCC's 'Data Protection Policy'
- KCC's 'Data Breach Policy' '
- KCC's 'Using IT Equipment for Remote Mobile Working - Policy & Standard'
- KCC's 'ICT Security information' pages on KNet.
- KCC's User Identification and Authentication Policy
- KCC's Work Smart (Flexible Working) – Guidance for Employees
- KCC's corporate e-learning and face-to-face training service provided via Delta
- Cantium Solutions 'Service Now' portal's 'Knowledge Base'

8. Advice and Support

If you are not clear about how you should use KCC's ICT equipment and/or systems, you can contact your line manager, Corporate Communications, the ICT Service Desk or the Human Resources Team.

9. Alternative Formats

This document is available in other formats. Call 03000 421553 or email alternativeformats@kent.gov.uk

10 Document Management

10.1 Review and Revision of this Policy.

This policy will be reviewed and, if necessary updated, as is deemed appropriate but no less frequently than every twelve months.

10.2 Ownership

Document Owner	
Version	**DRAFT** 0.1

10.3 Approvals

Version	Name	Job Title	Date of Issue