From mountain to sea

Aberdeenshire
COUNCIL

Mandatory Code of Practice:
Acceptable Use (IT)

Version 1.4

Implementation Date: 31 December 2020

1. Introduction

1.1 The Mandatory Code of Practice Acceptable Use (IT) *(hereinafter referred to as the **"MCOP"**)* sets out Aberdeenshire Council's *(hereinafter referred to as the **"Council"**)* approach to accessing IT Facilities. The Council recognises that access to IT Facilities is vital for the delivery of services and has developed policies, codes of practice and guidance to ensure appropriate and effective use of these facilities, covering all aspects of computer use, including email, internet and monitoring. Practical guidance and rules on the use of IT Facilities is provided in associated documents and standards which support this MCOP.

1.2 This MCOP is owned, managed and developed by the Council's Information Security Officer *(hereinafter referred to as the **"ISO"**)* on behalf of the relevant Head of Service overseeing the Council's IT function.

2. Scope

2.1. With the exceptions of pupils, the MCOP applies to everyone within the Council who accesses Council IT Facilities - devices, systems, technology, networks, telephony, databases, data and other resources. This includes all staff, Elected Members, contractors, visitors, consultants and any third parties engaged to support Council activity and who have authorised access to any IT Facilities *(hereinafter referred to as **"Users"**)*.

2.1.1. Councillors

2.1.2. Following their election, Councillors will be granted access to IT Facilities and other secure networks such as the Public Services Network *(hereinafter referred to as **"PSN"**)*, where these are required to enable them to fulfil their responsibilities as a Councillor. Access to Council IT Facilities is provided for Councillors to use in their three roles of Elected Member of the Council, Ward Representative and Political Party / Independent Member.

2.1.3. Councillors are required to act in accordance with the Council's requirements when using Council resource. IT Facilities must not be used for purely political purposes but may be used where part of the purpose could reasonably be regarded as likely to facilitate or be conducive to the discharge of the functions of the Council or of an office to which the Councillor has been elected or appointed to by the Council. Constituency work is regarded as proper use of IT Facilities.

2.1.4. The Council is prohibited by law from publishing any material of a party political nature. If a Councillor uses IT Facilities for the preparation of material of a party political nature in pursuance of Council duties, they must do so in a way which is not attributable to, or appears to be on behalf of, the Council. No costs should be incurred by the Council as a consequence of publication of any party political material by a Councillor using IT Facilities.

2.1.5. Councillors must not use IT Facilities provided to them in a manner which will prevent or interfere with its primary purpose as a facility to assist in the discharge of the functions of the Council. Accordingly, the Councillor must not:

- misuse IT Facilities in such a manner as to cause it to cease to function; and
- install or use any equipment or software which may cause IT Facilities to malfunction

2.1.6. Councillors shall make reasonable arrangements for the safe-keeping of any Council supplied IT equipment. This includes, but is not limited to laptops, tablets and mobile phones.

2.1.7. In addition to the rules set out in this Policy, Councillors must also abide by the rules surrounding IT in the Standards Commission for Scotland Councillors' Code of Conduct (and any amendment thereof or replacement thereto). These rules are currently defined under *"Use of Council Facilities*".

3. Purpose

3.1. The purpose of this MCOP is to provide Users with instructions and guidance on appropriate use of information technology including, but not limited to, laptops, tablets, mobile phones, email and Internet use. It supports the need of the Council to keep its IT Facilities – devices, systems, technology, networks, telephony, databases, data and other resources – in a safe and effective operational state so as to ensure the Confidentiality, Integrity and Availability of the information it processes. The main objectives of this MCOP 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.

- IT Facilities are protected in a cost effective manner;
- all Users of IT Facilities are aware of their responsibilities under this MCOP and associated Policies and guidance.

4. Overview

4.1. Authorised Users will be granted access rights to IT Facilities that are appropriate to their business requirements. No other unauthorised IT Facilities must be used. It is a criminal offence under the Computer Misuse Act 1990 to deliberately attempt to access a system which a User has no authority to access.

4.2. Access to IT Facilities is taken as acceptance of this MCOP and that all use of IT Facilities shall comply with relevant legislation.

4.3. The Council cannot recover information that is stored on Council supplied IT Equipment (e.g. the 'C Drive' of a laptop) if the device is lost, damaged or stolen. Users should, wherever possible, store and access files through the network rather than local storage. Notwithstanding this, information may be synced to the device to ensure that your information remains accessible in the event that network access is unavailable.

4.4. Council information must not be stored on non-Council supplied equipment or a personal hosted storage service, such as Dropbox, iCloud, Amazon, etc. Information stored in these services may not be held in countries allowed by prevailing legislation, and may put the User and Council at risk of breaching the law.

4.5. While access to Council supplied IT Equipment is provided for business use, reasonable personal use may be undertaken. Any personal use must be undertaken in compliance with relevant Council policies and must not interfere with normal business or be detrimental to productivity.

4.6. The Council may require access to Council supplied IT equipment at any time during normal office hours and you must allow such access.

4.7. The Council retains full ownership over any Council supplied IT Equipment and may ask for this to be returned at any point. Failure to return Council supplied IT Equipment upon request will be considered as theft.

4.8. Information created or collected as part of working for the Council is the property of the Council.

5. Compliance / Review

5.1. This MCOP is reviewed on a periodic basis by the ISO to ensure it remains accurate, relevant and fit for purpose. Such changes and revisions may be made by the ISO without further Committee approval for as long as such changes and revisions do not significantly alter the meaning or essence of this MCOP.

5.2. All Users with access to IT Facilities have a responsibility to comply with this MCOP and to promptly report any suspected or observed security breach to the ISO.

5.3. Failure to meet any of the requirements detailed within this MCOP may result in the User being subject to formal disciplinary action that will be dealt with under the appropriate disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under UK or Scots law, this may also be reported to Police Scotland or another appropriate authority.

5.4. 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 will take such punitive action against that User and/or their employer as the Council, at its absolute discretion, deems appropriate.

5.5. The Council reserves the right to take short term preventative action which protects the Council's IT Facilities, including but not limited to suspending a User's access.

6. Malware Control

6.1. Malware in the context of this MCOP is the term applied to all malicious software - that is software that attempts to damage, extort or otherwise abuse IT Facilities and Council data.

6.2. The Council seeks to minimise the risks of computer malware through education, procedures and anti-malware software. It is a crime under the Computer Misuse Act 1990 to deliberately introduce malicious programs into the network or server.

6.3. With the exception of mobile phones, all Council supplied equipment has approved anti-malware software installed and this is scheduled to be updated at regular intervals. Users need to ensure that the anti-malware software is being updated on their devices and must report any problems to the IT Service Desk.

6.4. Users of Council supplied IT Equipment must be aware of the risk of viruses from email, Internet and any removable devices. Users must never download files from unknown or suspicious sources, or allow software to be installed that has not been supplied by the Council. All Junk emails should be deleted and suspicious attachments must not be opened. Please refer to the Council guidance on Handling Junk & Phishing Emails.

6.5. The Council will take measures to prevent malware from entering the Council environment. There may, however, be cases where such measures will not detect a malware and the Council may subsequently need to access a User's device or email account to remove the malware without prior notice. Any such access or investigation will be carried out by an appropriate and competent member of the relevant IT Team under the guidance of the ISO.

6.6. Malware is capable of spreading from infected IT Equipment through the Council network and infect other IT Facilities without further User interaction. Therefore, where a User suspects that IT Equipment may have been infected with malware, Users must immediately disconnect the IT Equipment from the Council Network and remove any peripherals that may be plugged into IT Equipment and contact the IT Service Desk. Under no circumstances must Users re-connect the IT Equipment to the Council Network unless cleared to do so by the IT Service Desk.

7. Access Control

7.1. Access to IT Facilities is reserved for the business of the Council. Unauthorised use will be investigated, and if found to be an offence under the Computer Misuse Act 1990 may be reported to Police Scotland or another appropriate authority.

7.2. Users are given a unique Username to access IT Facilities and must create, manage and protect their passwords in accordance with the Mandatory Code of Practice on Passwords.

7.3. Users are required to screen-lock their IT Equipment when moving away from it and turning their IT Equipment off when transporting it outside the office. Unsecured IT Equipment must never be left unattended. It is the User's responsibility to ensure that adequate safeguards are taken to protect IT Facilities.

7.4. IT Facilities are only permitted to be used by authorised individuals. The Council may authorise personnel from other organisations to access Council systems by specifying acceptable usage in applicable contracts or agreements. Third party access will not be granted until contracts or agreements are finalised and signed.

7.5. Users working via a device that is not owned or issued by the Council shall do so in accordance with the Council's Information Security Framework as set out in the Information Security Policy, Mandatory Code of Practice Bring Your Own Device (BYOD) and the Council’s Mandatory Code of Practice Acceptable Use (IT) and any associated guidance and procedure.

7.6. Users working via a device that is owned or issued by the Council) shall do so in accordance with the Council’s Information Security Framework, Mandatory Code of Practice Acceptable Use (IT) and any associated guidance and procedures.

7.7. Working remotely can pose several security risks. To help reduce these risks, Users must do the following:

- take steps to ensure that the environment in which they work offers a suitable level of privacy and that other individuals cannot view papers or screens or overhear work related conversations;
- take precautions to safeguard the security of any equipment on which they do Council business, and keep their passwords secret;
- inform the the IT Service Desk and the ISO as soon as possible if any sensitive paperwork or Council supplied IT Equipment has been lost or stolen;
- inform the ISO and DPO as soon as possible if any personal identifiable information has been lost or stole or wrongfully disclosed;
- ensure that any work they do remotely is saved on the Council’s network or is transferred to it as soon as possible;
- wherever possible, avoid open public Wi-Fi where no password is required and always connect through the Council’s VPN client;
- ensure that encrypted memory sticks are kept separate from IT Equipment when not in use;
- ensure that IT Equipment is not left in view on public transport or left unattended in vehicles;
- unless absolutely necessary, do not access, work with or work on information that are classed as “OFFICIAL - SENSITIVE”, “SECRET” or “TOP SECRET” in public places; and
- Do not leave papers or equipment containing “OFFICIAL”, “OFFICIAL - SENSITIVE”, “SECRET” or “TOP SECRET” information unattended and ensure that they are properly protected from theft or unauthorised access.

7.8. No attempt must be made to switch off or bypass IT Security Controls, including, but not limited to, firewall or anti-malware systems.

7.9. Ensure that information is backed up by saving it within SharePoint, OneDrive or the Council’s Records Management System.

7.10. Wherever possible, ensure that information is classified according to the Council's approved Information Asset Classification scheme (PUBLIC, OFFICIAL, OFFICIAL - SENSITIVE, SECRET, TOP SECRET).

7.11. Adopt good cyber resilience housekeeping practices to ensure IT Facilities, documents and information are well protected at all times and that documents and information are safely destroyed in accordance with the Council's Records Retention Schedule.

7.12. Understand responsibilities for retention of documents and information to comply with legal requirements.

7.13. Take appropriate measures to ensure the safekeeping of hardware, especially laptops, external storage devices, tablets, and other mobile devices. Council supplied IT Equipment must not be left unattended in cars, public transport, hotels or other public places when logged in.

7.14. Users must contact the IT Service Desk in order to:

- dispose of any Council supplied IT Equipment;
- purchase IT Equipment for business use;
- install, uninstall or amend any software not available through the Software Centre;
- subscribe to, purchase or otherwise use any third party hosted or cloud based system not available through the Software Centre;
- copy Council licensed software from one device to another;
- report the loss or theft of a device; or
- report faults or failures of a device.

7.15. IT Equipment is identified by an asset tag and a unique asset number, Users must not remove this identification or tamper with it.

8. Email Use

8.1. Council email must not be used to discredit or embarrass the Council, be used for illegal activities or otherwise break any law or convention.

8.2. Users must not amend or delete the automatic footer that is attached to all external emails.

8.3. Users must never distribute pornography, send or receive illegal material (including unlicensed software) or forge a message to make it appear to have originated from another person.

8.4. Email must be used in a positive, supportive, respectful way and:

- must not include defamatory, rude or abusive language;
- must not be used to harass, annoy or intimidate an individual or group of individuals;
- chain mail, jokes, spam, animations or hoax virus warnings must not be shared with individuals or groups using Council email systems.

8.5. Users must not represent themselves or others by using extracts from another person's message without appropriate acknowledgement.

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

8.7. While Users will not be held responsible for receiving objectionable material in unsolicited email, they must either:

- refer the email to a line manager for appropriate action where the email is potentially illegal or offensive. This may then be escalated to the Council's ISO as appropriate; or
- where the email is unlikely to be illegal or offensive, Users must immediately delete the email, without forwarding it to anyone.

8.8. Email should be used in line with the requirements of the Council's Information Asset Classification scheme (PUBLIC, OFFICIAL, OFFICIAL - SENSITIVE, SECRET, TOP SECRET) and Guidance on Using Email Securely.

8.9. Confidential, personal or sensitive data must be managed in accordance with General Data Protection Regulations (and any amendment thereof or replacement thereto) and the Data Protection Act 2018 (and any amendment thereof or replacement thereto).

8.10. Users must treat email received from unknown or unexpected sources with caution and not click on any links or open any attachments unless it is safe to do so.

8.11. Users must handle Junk and Phishing emails in accordance with the Council's Guidance on Handling Junk & Phishing Emails.

8.12. Users must not set up automatic forwarding of emails to an external email address or a personal email address.

8.13. Users must not forward Council email or Council owned information to their personal email address unless there is a valid business need that is appropriate to the User's job role and

(i) the information is not personal identifiable information as defined under Section 3 (2) of the Data Protection Act 2018 *(and any amendment thereof or replacement thereto)*, or

(ii) the information is not otherwise sensitive or confidential or

(iii) the information is not classed as "OFFICIAL - SENSITIVE", "SECRET" or "TOP SECRET".

8.14. Distribution of Council-wide email will take place only in exceptional circumstances and must be approved by the Head of Service (Customer & Digital). This will only be considered when the information is of a significant urgent nature with relevance to all employees and requires immediate action.

8.15. Email is not a records management system. Information and records received by email must be stored in an appropriate location, outwith the email system in order to ensure continued availability.

8.16. Personal email sent to a User's work email address is subject to the same degree of filtering and monitoring as business email and there can be no presumption of privacy.

9. Internet Use

9.1. Internet access is provided for business use. Its use must comply with current legislation, Council policy and rules and must not create business risks to the Council through misuse.

9.2. All actions undertaken while using the Internet will be attributed to the User logged into the IT Equipment.

9.3. Users must not browse the Internet from IT Equipment they have not logged into.

9.4. Information or images from the Internet must not be used for Council business in violation of Copyright and Intellectual Property Rights legislation.

9.5. Users must not participate in any form of Internet misuse while using a Council device, including but not limited to:

- illegal activity;
- personal business activity;
- on-line gambling sites;
- dating sites;
- the use of personal on-line storage systems.

9.6. Users must not deliberately attempt to access offensive material. Any unintended access of any site that are clearly offensive should be reported to the IT Service Desk so the web filter can be updated accordingly.

9.7. Users must exercise caution when browsing unfamiliar websites. Compromised websites may be used to trick users into activating malware.

9.8. Report any messages generated by anti-malware software to the IT Service Desk immediately.

9.9. Users must not post messages or images on any Internet message board or other similar web based service that would bring the Council into disrepute. Publishing defamatory and/or knowingly false material about the Council, colleagues or our customers on social networking sites, blogs, wikis, twitter or any online publishing format is prohibited.

9.10. Users must not host a personal website on any Council supplied IT Equipment.

9.11. Users must only register Council email addresses on business related websites.

9.12. Internet access is provided to conduct Council business. Users must remain vigilant about security and availability for others when using the Internet.

9.13. Personal use of the Internet using Council supplied IT Equipment or the Council network is permitted as long as it does not impact the performance or security of the council network, or the delivery of normal work activities. Any personal use must comply with Council standards.

9.14. No attempt must be made to by-pass or modify internet restrictions imposed by the Council.

9.15. Users must seek approval from the ISO as well as their line manager before requesting the lifting or relaxing of Internet controls.

9.16. Downloading large files for personal use, such as music or video, is not permitted.

9.17. All Internet access may be monitored and logged. The Council may access and report on this information. Monitoring may identify individuals, the dates and times of their Internet use, together with details of the sites accessed. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

10. IT Monitoring

10.1. By logging on to any Council IT Facility, a User is consenting to the Council's monitoring procedures.

10.2. 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;
- review usage.

10.3. To ensure information processing systems are not open to abuse, the Council reserves the right to monitor Users' usage. This level of monitoring will be fair and proportionate and must be authorised by the ISO.

10.4. Monitoring differentiates between:

- **Usage logging:** Collecting data, generally from system log files about how and when a User accessed and used IT equipment; and
- **Content inspection:** Viewing information held in business or personal files, email or on screen.

10.5. Usage logging ensures and improves service performance and helps identify and investigate potential prohibited use or misuse.

10.6. Content inspection will only be undertaken for legitimate business reasons which may include, but is not limited to:

- investigation of a potential cyber security breach;
- investigation of any potential breaches under this MCOP;
- to comply with the request of law enforcement officers;
- to comply with legal obligations;
- to prevent or detect contravention of criminal or civil law; and
- investigation of a potential breach of an individual's employment contract.

10.7. Content inspection may involve, but is not limited to, viewing information held in:

- business and/or personal files and documents;
- business and/or personal email messages or any other IT based communication;
- business and/or personal information displayed on a screen;
- emails that have not yet been opened or received by the intended recipient.

10.8. The ISO may, at his discretion and only in exceptional circumstances, initiate an investigation that relies on usage logging and/or content inspection. Where the investigation involves a Head of Service, the ISO must inform the relevant Director of such investigation. Where the investigation involves a Director or Elected Member, the ISO must inform the Chief Executive of such investigation. Where the investigation involves the Chief Executive, the ISO must inform Elected Members.

10.9. Managers will require authorisation from a third-tier manager **and** the ISO to initiate an investigation that relies on usage logging and/or content inspection. Where the request involves a Head of Service, authorisation must come from a Director **and** the ISO. Where the request involves a Director or Elected Member, authorisation must come from the Chief Executive **and** the ISO. Where the investigation involves the ISO, authorisation must come from the relevant Head of Service responsible for IT **and** a Director.

10.10.Other than in exceptional circumstances, the individual concerned will be informed of any inspection in advance and again on completion. The Council recognises, however, that in certain circumstances it may be necessary to obtain access without informing the individual. The ISO will, upon considering all the facts, decide whether it is appropriate to inform the individual concerned about any inspection. The ISO's decision is final.

11. Responsibilities

11.1. Each Team Leader or Line Manager must ensure Users within their area of responsibility fully understand this MCOP and must report any misuse to the ISO as soon as they become aware.

11.2. All Users will:

- know and comply with this MCOP;
- use and manage technology resources responsibly;
- be accountable for their actions relating to this MCOP;
- report unusual email activity to the IT Helpdesk.

12. Associated Standards Legal Provisions

12.1. Legislation

12.2. There are a number of pieces of legislation relevant to this MCOP. A non-exhaustive list of relevant statutory provisions is below

12.2.1.The **Computer Misuse Act 1990** (and any amendment thereof or replacement thereto). Under this Act:

- 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.

12.2.2.The **Data Protection Act 2018** (and any amendment thereof or replacement thereto) and **Regulation (EU) 2016/679,** more commonly known as the **General Data Protection Regulation** (and any amendment thereof or replacement thereto) *(hereinafter referred to as the **"GDPR"**)* sets out what may or may not be done with personal data. It states that it is an offence to obtain knowingly or recklessly, disclose, or procure the disclosure of personal information without the consent of the data controller. The offence is punishable by various means and could lead to significant fines. Further advice and guidance is available on the Council's Data Protection Page.

12.2.3.The **Freedom of Information (Scotland) Act 2002** (and any amendment thereof or replacement thereto) gives individuals a right of access to information held by the Council, subject to a number of exemptions and advice and guidance is available on the Council's Freedom of Information & Environmental Information Page.

12.2.4.The **Environmental Information (Scotland) Regulations 2004** (and any amendment thereof or replacement thereto) governs access to environmental information held by the Council and requires the Council to publish environmental information, and make it available on request. Further advice and guidance is available on the Council's Freedom of Information & Environmental Information Page.

12.2.5.The **Copyright, Designs and Patents Act 1988** (and any amendment thereof or replacement thereto) governs the use of a 'work' created by an individual or company.

12.2.6.Other relevant legislation include, but are not limited to:

- Civil Evidence (Scotland) Act 1988 (and any amendment thereof or replacement thereto);
- Copyright (Computer Programs) Regulations 1992 (and any amendment thereof or replacement thereto);
- Freedom of Information (Scotland) Act 2002 (and any amendment thereof or replacement thereto);
- Human Rights Act 1998 (and any amendment thereof or replacement thereto);
- Counter Terrorism and Security Act (2015); Prevent Guidance (and any amendment thereof or replacement thereto);
- Official Secrets Act 1989 (and any amendment thereof or replacement thereto);
- Criminal Procedure (Scotland) Act 1995 (and any amendment thereof or replacement thereto);
- Public Records (Scotland) Act 1937 (and any amendment thereof or replacement thereto);
- Public Records (Scotland) Act 2011 (and any amendment thereof or replacement thereto);
- Regulations of Investigatory Powers (Scotland) Act 2000 (and any amendment thereof or replacement thereto);
- Serious Organised Crime and Police Act 2005 (and any amendment thereof or replacement thereto);

- The Civil Contingencies Act 2004 (and any amendment thereof or replacement thereto);
- The Communications Act 2003 (and any amendment thereof or replacement thereto);
- The Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000 (and any amendment thereof or replacement thereto);
- Wireless Telegraphy Act 2006 (and any amendment thereof or replacement thereto) and
- Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments Regulations) 2002 (and any amendment thereof or replacement thereto).

12.3. Policies

12.3.1. Information Security Policy (and any amendment thereof or replacement thereto);

12.3.2. Social Media Procedure (and any amendment thereof or replacement thereto);

12.3.3. Data Protection Policy (and any amendment thereof or replacement thereto).

12.4. Mandatory Codes of Practice

12.4.1. Passwords (and any amendment thereof or replacement thereto)

12.4.2. Remote Working (and any amendment thereof or replacement thereto);

12.4.3. Information Asset Classification (and any amendment thereof or replacement thereto).

12.4.4. IT Asset Management (and any amendment thereof or replacement thereto);

12.5. Guidance:

12.5.1. Secure Email (and any amendment thereof or replacement thereto);

12.5.2. What is Confidential Information (and any amendment thereof or replacement thereto);

12.5.3. Mail Procedure (and any amendment thereof or replacement thereto).

13. Definitions

13.1. **Confidentiality:** Information is not made available or disclosed to unauthorised individuals, entities or processes.

13.2. **Integrity:** Information's accuracy, validity and completeness is protected.

13.3. **Availability:** Information is accessible and usable upon demand by an authorised entity.

13.4. **IT Facilities:** IT Stands for "Information Technologies” and refers to technologies that provide access to information. IT Facilities is an umbrella terms and refers to devices or IT Equipment, systems, technology, networks, telephony, databases, data and other resources and for the purpose of this MCOP will include any personal device that has been enrolled as BYOD (Bring Your Own Device) when used to access Council information.

13.5. **IT Equipment:** This refers to any IT hardware such as servers, BYOD devices and IT hardware that has been provided to a User for a particular purpose, including, but not limited to laptops, tablets, and mobile phones.

13.6. **Peripherals:** This refers to any hardware device, such as an external hard drive or USB Flash Driver which connects to the computer.

13.7. **IT Security Controls:** These are safeguards or countermeasures to avoid, detect, counteract, or minimise security risks to IT Facilities or the Council’s information assets.

— END OF MANDATORY CODE OF PRACTICE —

Version Control

Version	Date	Author	Description
0.1	28/01/2020	Lars Frevert	Document creation and draft as a result of Para. 2.1.6 of Internal Audit Report 1932 *“Data Security in a Cloud Based Environment”.* Approved by ITSMT to progress to formal consultation stage.
0.2	31/03/2020	Lars Frevert	Submitted to HR to pass to Trade Unions and key managers for comment / feedback.
0.3	25/06/2020	Lars Frevert	Draft document updated following feedback from consultation with Trade Unions and key managers.
1.0	01/09/2020	Lars Frevert	Draft document placed before Area Committees between 18/08/2020 and 01/09/2020 for review and comment with proposal to replace current Acceptable Use Policy, Acceptable Use ICT Code of Practice, Use of ICT Facilities by Employees, Use of ICT Facilities by Elected Members, Monitoring and Investigation of ICT Facilities
1.1	01/09/2020	Lars Frevert	Draft document updated following feedback from the Marr, Banff & Buchan, Buchan, Garioch, Kincardine & Mearns and Formartine Area Committees with view of placing final document before the Business Services Committee.
1.2	15/10/2020	Lars Frevert	Name changed to Mandatory Code of Practice Acceptable Use IT. Draft document finalised in order to be placed before Business Services Committee on 12 November 2020 for approval.
1.3.1	22/12/2020	Lars Frevert	Pursuant to Para. 5.1, changes made to Para. 8.13 to clarify position in relation to forwarding Council email to a personal email address. Changes approved by Head of Customer & Digital Services on 23 December 2020.

Approval

Version	Date	Authority	Approval Comments
1.3	12/11/2020	Business Services Committee	Business Services Committee formally approved Mandatory Code of Practice - Acceptable Use IT on 12 November 2020. Mandatory Code of Practice - Acceptable Use IT (v. 1.3) implemented on 30 November 2020.
1.4	31/12/2020	Head of Service Customer & Digital Services	Following feedback after the publication of the Mandatory Code of Practice - Acceptable Use IT, the Head of Service for Customer & Digital Services formally approved changes to Para. 8.13. Mandatory Code of Practice - Acceptable Use IT (v. 1.4) implemented on 31 December 2020.