Ref. No.	CO/IG/5
Category:	
People	
Place	
Corporate	Yes
In Constitution	

ICT Acceptable Use Policy

Policy Details

What is this policy for?	This is a policy which all users of new Dorset Council ICT equipment, infrastructure and services are required to comply with. It is associated with (i) Information Security policy (ii) Email security policy and (iii) Social media use policy.
Who does this policy affect?	All members of staff including Members, contractors and suppliers who use any person who uses any Dorset Council ICT.
Keywords	Computer Misuse, IT use, ICT use, telephony use, Skype use, Laptop use, Tablet use, Smartphone use, GDPR, Data protection, data breach, acceptable use, unacceptable use.
Author	John McGarvey, Senior Business Analyst, Shaping Dorset Council Programme (in association with Lucy Williams, ICT Service Delivery Lead (EDDC) and James Ailward ICT Service Delivery Works-Package Lead.
Does this policy relate to any laws?	• Communications Misuse Act 1988 • Computer Misuse Act 1990 • Freedom of Information Act 2000 • Copyright and Related Rights Regulations 2003 • Communications Act 2003 • Data protection Action 2018 (brings the GDPR into UK law).
Is this policy linked to any other Dorset Council policies?	(i) Information Security policy (ii) Email security policy and (iii) Social media use policy. These first two documents contain specific information of a more technical nature and security nature.
Equality Impact Assessment (EqIA)	The EqIA screening assessment required a new EqIA to be carried out.
Other Impact Assessments	No known budget issues. There is a reputational risk if unacceptable use of ICT by Dorset Councils staff, its contractors, customers and/or suppliers is not prevented. To mitigate the risk, new staff are trained on induction, IS Security is dealt with in a separate policy document.

Status and Approvals

Status	Live	Version	1
Last review date	March 2019	Next review date	
Approved by (Director)	Dorset Council Corporate Director: Legal and Democratic	Date approved	27 March 2019

Appendix 3

ICT Acceptable Use Policy

v1.0 Approved

Purpose	This document will be the ICT acceptable use policy established to provide guidelines for the conditions of acceptable and appropriate use of computing and networking resources provided by Dorset Council.
Scope	This policy encompasses all users and aspects of the Council's computer systems. The policy applies to all elected members, employees, contractors, suppliers, third parties consuming ICT services from Dorset Council (e.g. Tricuro) and any person who directly uses Dorset Council ICT services or information systems used for Dorset Council purposes. The AUP does not extend to individuals using public Wi-Fi on personal devices. This policy applies whenever users access the Council's computer systems, telephony and related resources including ICT equipment, systems, connections and extends to externally contracted entities and partners.

Table of contents
Table of contents

With paragraph headings and page numbers. Use simple, clear headings, with internal links to the rest of the document for ease of navigation.

Glossary

Explaining any abbreviations, acronyms, technical terms and unavoidable jargon.

1. Introduction

1.1. Dorset Council encourages the use of electronic communications to share information and knowledge in support of its business. Accordingly, facilities such as telephony, instant messaging, presence information, voicemail, teleconferencing, video conferencing, email, intranet, internet, electronic storage and collaborative working services are subject to this policy where they are provided.

1.2. These communications services rely on voice and data networks delivered over both physical and wireless infrastructures. Digital technologies are unifying these communications functions and services, blurring traditional boundaries. This Policy recognises this and establishes an overall policy framework for electronic communications.

1.3. It also establishes new policy and procedures replacing those of the sovereign authorities and this Policy defers to other Council policies or procedures where relevant.

1.4. However, it is recognised that an integrated policy cannot anticipate all the new issues that might arise in electronic communications. One purpose of this Policy is therefore to provide a framework within which these new issues can be resolved.

2.0 Overview

2.1 This Acceptable Use Policy (AUP) is not intended to impose restrictions on users. It is intended to protect staff, the Council's customers and the organisation itself from the inappropriate use or sharing of its systems, networks and information, either knowingly or unknowingly, by outlining the type of behaviour expected of those using technology in the workplace and the consequences of abusing the privileges given to them.

2.2 It is the responsibility of every computer user to know this policy and to conduct their activities accordingly.

2.3 This policy is available from the new Dorset Council corporate intranet.

3.0 General Principles for Use and Ownership

3.1 IT security is the responsibility of the Council as a corporate entity and a personal responsibility for all members of staff who use computer equipment and systems. For security and network maintenance purposes, authorised individuals within Dorset Council ICT Department may monitor equipment, systems and network traffic at any time.

3.2 The Council reserves the right for Chief Officers or their designated officers to authorise the checking and auditing of networks, systems, devices and the information processed on them on a periodic basis to ensure compliance with this policy.

3.3 The Council must adhere to all UK legislation affecting ICT and information processing. All staff must comply with the following Acts and may be held personally responsible for any breach of current legislation as listed below and any future legislation that may be enacted:

- Communications Misuse Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyright and Related Rights Regulations 2003
- Communications Act 2003
- The Data Protection Act 2018 introducing the UK's implementation of the GDPR.

3.4 All computer data relating to living individuals is covered by Data Protection legislation. Where such data is held, then the provisions of that legislation must be followed.

3.5 Official Council equipment, including portable and laptop computers, shall be used for official purposes only, except where personal use does not infringe the terms of the Information Security Policy or the discrete policies within the overarching framework. Private material should not be stored on Dorset Council owned equipment or network drives.

3.6 Computing equipment is extremely sensitive and great care must be taken to avoid accidental damage. Eating or drinking close to such equipment should be avoided.

3.7 Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and music files, video and video files, and the installation of any copyrighted software for which Dorset Council or the end user does not have an active license is strictly prohibited.

3.8 Chief Officers are responsible for the security and proper use of computer equipment within their directorates, including establishments. Where they designate specific officers responsible for specific equipment and systems, then such delegations must be recorded, and that record must be kept up to date.

3.9 Data Breach

3.10 All known or suspected ICT security breaches or threats must be reported to the ICT Service Desk at the earliest opportunity.

3.11 Personal data breaches must be reported to the data protection team. The procedures covering this are outlined in the Dorset Council **Information Security Management Policy**.

4.0 Personal and Access Security

4.1 Accepted Use

4.1.1 Users of computers connected to the Dorset Council network must lock-up from the network at the end of the day. Computers should be locked when unattended.

4.1.2 ICT equipment such as desktop computing facilities or laptop/tablet computer should not be left unattended unless locked or logged out. If the use takes a break or leave the device unattended, it must be left 'locked' (depress window symbol and 'L') to secure it.

4.1.3 All PCs, laptops and workstations are built secured with a password-protected screensaver with the automatic activation feature. Users may not interfere with this setting.

4.1.4 For security purposes, access to computing and network resources is via individual accounts and passwords. Authorised users are responsible for the security of their passwords and accounts in accordance with the Password Standard. If it is necessary to disclose a password to ICT Staff for system maintenance or software installation etc. then that password should be changed as soon as possible.

4.1.6 All documents and media containing sensitive or protectively marked information must be kept securely out of plain sight when not in use as per the **HMG protective marking policy**

4.1.7 Controlled stationery must be held security. E.g. Blank cheques, security tags etc.

- 4.1.8 Where data or systems are kept on portable media, then such media must be encrypted in accordance with Dorset Council policy. Personal drives (e.g. P: or G: drives) are for personal, work-related information only, such as completed appraisal forms or personal notes from a training course.
- All other work-related data and documents must be kept in a shared drive (e.g. H: S: or T: drive) or system with shared access. Please select the appropriate area carefully according to the permissions required and avoid storing documents needed by other members of your team in a personal area where they cannot access it.
- Files should not be kept on hard drives of devices or on external hard drives. Data held here is not backed up and will be lost in the event of a failure. It will also not be transferred to a new machine when the device is replaced.

4.1.9 Back-up media should be kept locked away and separate from the location of the originals. Data and software held centrally by IT Services will be secured by them. Only persons authorised to do so may gain access to secure areas.

4.1.10 The transfer of "means of access" (e.g. keys, cards, electronic fobs) or disclosure of access codes to unauthorised personnel is strictly forbidden. The loss of "means of access" (e.g. keys, cards, electronic fobs) must be reported immediately so that necessary action can be taken to ensure to codes are cancelled or changed.

4.1.11 Persons leaving the employment of the Authority must return all "means of access", identity cards, manuals and any other property of the Council to their line manager by their last working day. Line Managers are responsible for notifying HR and IT to ensure that user accounts are closed or cancelled at the same time.

4.1.12 All media of uncertain or unreliable origin must be checked for viruses before the media is accessed using Council computers. Where a virus is detected, the matter must be reported to the ICT Service Desk immediately.

4.2 Software

4.2.1 Only officially approved software may be installed, and then only by IT Services staff, to be run on any resources owned or supported by DCC. In this context, "officially approved" refers to software applications that are supported or approved by IT services.

4.2.2. Members using a Corporately Supplied Personally Enabled (COPE) device are permitted to install properly licensed software to support either wider democratic/community roles or personal requirements. ICT Service Desk cannot to support these products.

4.2.3 Only IT Services staff should install, modify, or update software installed on any IT resources owned or supported by DCC, except where preauthorised software update processes are enabled. The use, or possession of unlicensed copies or "pirated" versions of software is illegal and therefore, expressly prohibited.

4.2.5 All computer software developed for Dorset Council is for the sole use of the Council.

4.2.6 Users must not duplicate any licensed software or related documentation for use either on Council premises or elsewhere unless Dorset Council is expressly authorised to do so by agreement with the licensor.

4.2.7 No employee should give any company software to any outsiders, including customers and clients.

4.2.8 All software, information and programs developed for and/or on behalf of the Council by employees during their employment remain the property of the Council.

4.2.9 All Dorset Council computers have the standard anti-virus software installed. Settings on this software are password protected and must not be changed at any time unless authorised by ICT Services personnel.

4.3 Internet Usage

4.3.1 Internet access is provided for official business. Personal use of the corporate internet connection by staff is permitted but this must be in their own private time and at no extra cost to the Authority. All traffic via the corporate internet connection is logged and will be subject to monitoring without prior notice.

4.3.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use of the Internet. Official Council equipment is provided for official use only, except where specifically permitted.

4.3.3 Viewing or transmission of any material which may be regarded as offensive or in violation of any UK law or regulation is not permitted. Such material may include, but is not limited to, copyright material, material judged to be threatening, sexually explicit or obscene and material protected by trade secret.

4.3.4. Internet filtering software has been put in place on all outgoing internet connections from the council to prevent access to inappropriate sites. Any occasions where users have been able to access to any inappropriate site(s) shall be reported to the ICT Service Desk so that the site(s) can be blocked.

4.4 Government Public Services Network (PSN)

4.4.1 Users of the PSN are responsible for any use of the PSN using their unique credentials.

4.4.2 Unique PSN credentials must not be shared between users and equally must not be used to access the PSN by anyone other than the owner of those credentials.

4.4.3 The PSN must only be accessed from those ICT systems and locations that have been explicitly authorised for this use.

4.4.4 Email must not be auto-forwarded from any email account to any other external email account.

4.4.5 Users are required to protect any sensitive or not protectively marked material sent, received, stored or processed via the PSN as appropriate. Protectively marked information may only be sent 'over the internet' using the corporate secure email system.

4.5 Telephony Systems Use

4.5.1 The use of Council telephony systems (e.g. Skype) creates transaction records (which include the number called and the time and length of the call) that are reviewed (when reviewed) by those authorised to do so as part of routine accounting procedures. Employees who use Dorset Council telephony for personal or other purposes should be aware that line managers have access to records of all calls made and that such records may be used for administrative purposes.

4.5.2 The only private phone calls which should be made during office time are those which cannot be made in users own time. Private calls should be made from the users own extension except when they are working away from their normal place of work.

4.5.3 Email and Communications activities

4.5.4 The Corporate email system is provided for official business. Personal use is permitted provided it does not violate the **Information Security Policy** and does not hamper or conflict with official business.

4.5.5 Dorset Council retains the right to view and monitor all email created, sent, forwarded, received or saved on the corporate email system without prior notice.

Users must always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain.

4.5.6 Users must send confidential, sensitive or personal information (sensitive and personal information are as defined by the Data Protection Act 2018) by secure email services provided for this purpose. Sending confidential, sensitive or personal information without such protection is prohibited.

4.5.7 Users must not open e-mail attachments received from unknown senders, which may contain viruses harmful to the ICT infrastructure and the security of its information.

4.5.8 Recipients of “chain email” should delete any such messages and attachments received and should not participate in the onward transmission of such material.

4.5.9 External/third-party email services (commonly known as “webmail”), such as Gmail, Hotmail, Yahoo or similar, must not be used for business purposes. Do not forward or auto-forward corporate email to external/third party email systems.

4.7 Printing

4.6.1 Network printing e.g. (‘Follow me’) printers are provided for official use. Users are encouraged to save resources and carefully consider the need to print copies of documents. It is accepted that some difficult to view documents may need to be printed because of their format (e.g. A3 tabulated lists or workflow diagrams). However, the printing of emails is discouraged unless needed for legal or other official reasons.

5.0 Unacceptable Use

5.1. The following activities are, in general, prohibited. Under no circumstances is an employee of Dorset Council authorised to engage in any activity that is illegal under UK or international law while using Dorset Council owned resources.

5.1.2 The list below is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

- Any form of harassment via email, telephone, SMS text, social media sites (for example, Facebook) or paging, whether through language, frequency, or size of messages;
- Visiting any website containing obscene, hateful or other objectionable materials;
- Any use of peer to peer/content sharing network software (e.g. Kazaa or BitTorrent) to transmit or access material into/out of the Dorset Council network infrastructure;
- Any use which involves a personal business venture;
- Deliberate introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.);
- Revealing or publicising of confidential or proprietary information which includes, but is not limited to: financial information, marketing strategies and plans, databases and the information contained therein, customer lists, computer software source code, and business relationships;
- Any personal use of Dorset Council resources that exceeds a reasonable duration or frequency, or interferes with the performance of the official duties of any other Dorset Council employee;
- Unauthorised sharing of computer accounts or loaning of passwords to other people;
- Any use contrary to *Criminal and Statutory Law*, *Copyright Law,* any other European or Government statute or regulation, or law, including any noncriminal statute or regulation.

6.0 Enforcement

6.1 If there is evidence to suggest that users have wilfully or negligently failed to abide by these policy requirements, Dorset Council has the right to investigate which may result in disciplinary action in line with the Council's disciplinary procedure.

7.0 ICT Security and Data Breaches

7.1 An ICT Security Breach is likely to have occurred when an unauthorised entity has (or is thought to have) gained access to one or more ICT systems. Examples of ICT Security Breaches would include but are not limited to:

- The loss of a laptop, tablet or mobile phone connected to the Council's network;
- Unauthorised access, or potential unauthorised access, to a user's account;
- Disclosing your password to someone else either intentionally or by accident;
- Malicious software (MalWare) is installed (or is thought to have been installed) on a PC, laptop, tablet or phone either intentionally or by accident.

Should a user believe that any of these situations may have occurred, they are to inform the ICT Service Desk immediately giving as much information as you can on the nature of the breach/suspected breach, time and potential users accounts involved. If you are in any doubt, report.

7.2 An Information/Data Beach may have occurred because of an ICT Security Breach but is not solely dependent on an ICT Security Breach. Examples that are not directly linked to a Security Breach would include.

- Sending a file or email to the wrong person;
- Accessing information either electronically or in paper form that you do not have a legitimate reason to access;
- Loss, or potential loss of information via any means;
- Unlawful disclosure of information.

Personal Data Breach is said to have occurred when personal information was disclosed due to any reason e.g. would include loss of a controlled paper file. These types of incident must be reported internally in accordance with the Council's Data Breach Policy. If you are in any doubt, report.