

**Policy Document**

**Information Security Policy Overview**

June 2018

**Contents**

[1 Introduction 3](#_Toc522186418)

[2 Purpose 3](#_Toc522186419)

[3 Information Security Policy Documents 4](#_Toc522186420)

[3.1 Email Policy 4](#_Toc522186421)

[3.2 Internet Acceptable Usage Policy 5](#_Toc522186422)

[3.3 Software Policy 5](#_Toc522186423)

[3.4 IT Access Policy 6](#_Toc522186424)

[3.5 GCSx Acceptable Usage Policy and Personal Commitment Statement 7](#_Toc522186425)

[3.6 Human Resources Information Security Standards 7](#_Toc522186426)

[3.7 Information Protection Policy 8](#_Toc522186427)

[3.8 Computer, Telephone and Desk Use Policy 8](#_Toc522186428)

[3.9 Legal Responsibilities Policy 9](#_Toc522186429)

[3.10 Remote Working Policy 10](#_Toc522186430)

[3.11 Removable Media Policy 11](#_Toc522186431)

[3.12 Information Security Incident Management Policy and Procedure 11](#_Toc522186432)

[3.13 Communications and Operation Management Policy 12](#_Toc522186433)

[3.14 IT Infrastructure Security Policy 13](#_Toc522186434)

[3.15 Bring Your Own Device (BYOD) Policy 14](#_Toc522186435)

[4 Policy Compliance 14](#_Toc522186436)

[5 Policy Governance 15](#_Toc522186437)

[6 Review and Revision 15](#_Toc522186438)

[7 References 15](#_Toc522186439)

[8 Personal Commitment Statement 16](#_Toc522186440)

# Introduction

In order to ensure the continued delivery of services to our customers, Chichester District Council is making increasing use of Information and Communication Technology (ICT) and customer information held by the Council and other public sector organisations.

The information that the Council holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected, maintain public confidence and the highest standards of information security.

# Purpose

This document provides a **summary** of the Information Security Policies developed by Chichester District Council. The objective of these policies is to ensure the highest standards of information security are maintained across the Council at all times so that:

* The public and all users of the Council's information systems are confident of the security, integrity and availability of the information used and produced.
* Business damage and interruption caused by security incidents are minimised.
* All legislative and regulatory requirements are met.
* The Council's equipment and facilities are used responsibly, securely and with integrity at all times.

The policies developed by Chichester District Council are based on industry good practice and include:

* Email Policy.
* Internet Acceptable Usage Policy.
* Software Policy.
* IT Access Policy.
* GCSx Acceptable Usage Policy and Personal Commitment Statement.
* Human Resources Information Security Standards.
* Information Protection Policy.
* Computer, Telephone and Desk Use Policy.
* Legal Responsibilities Policy.
* Remote Working Policy.
* Removable Media Policy.
* Information Security Incident Management Policy.
* Communications and Operation Management Policy.
* IT Infrastructure Policy.
* Data Sharing Policy
* BYOD Policy

Each of these detailed policies are available on the Intranet.

This document provides an overview of each of the individual policies, highlighting key messages that all members of staff need to be aware of when using electronic systems and sharing information with partner organisations. There are some references within these policies that apply only to particular service areas due to the nature of their work. Below is an explanation of what these phrases mean:-

GCSX email – This is a separate email facility that provides for a single secure data line between East Pallant House and central government for transmitting “Official – protect or official –sensitive”

‘Official Protect’ data includes but is not exclusive to:-

* Data that, if lost, could cause short term distress for an individual, e.g. loss of an individuals record containing personal data that could be used for criminal purposes e.g. bank account details.
* Data that if lost would breach statutory regulations such as the Data Protection Act.
* Contract or tender documentation.

 ‘Official Sensitive’ data includes but is not exclusive to:-

* Information relating to the award or withdrawal of a contract.
* Information that would prejudice the investigation of a crime.
* Policy advice to Ministers.
* Data that if lost could cause risk to a third party’s personal safety.

All staff are required to sign this policy document to confirm:-

* That they have read and understood these key messages.
* That they understand that failure to comply with these policies is a disciplinary offence.
* That they understand they have a responsibility under the terms of their employment to familiarise themselves with all Information Security Policies listed above.

# Information Security Policy Documents

## Email Policy

Policy Statement

Chichester District Council will ensure all users of Council email and Instant Message facilities are aware of the acceptable use of such facilities.

Key Messages

* This policy applies to all digital forms of communication; email, and IM
* Emails are automatically deleted within 90 days, IM are not held centrally and any messages will be held until all parties have deleted their local copy
* Staff must make every effort to ensure that the confidentiality of email and IM are appropriately maintained.
* Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies
* All emails that are used to conduct or support official Chichester District Council business must be sent using a “@chichester.gov.uk” address.
* All emails sent via the Government Connect Secure Extranet (GCSx) are of the format “@chichester.gcsx.gov.uk”.
* An email has the same legal status as a paper document and may be disclosed under the Data Protection Act 2018 or the Freedom of Information Act 2000. Further information on this can be obtained from the Data Protection Policy or by contacting the Council’s Data Protection Officer.
* Staff and Councillors **must not use** non-work email accounts to conduct or support official Chichester District Council business.
* Set out of office replies for absences longer than one day
* Use BCC rather than CC to multiple recipients.
* All official external e-mail must carry the official Council disclaimer (see section 6.1).
* Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s Equal Opportunities policy.
* Although all emails received are virus scanned, if you receive an email from a suspicious source or with an odd or unexpected subject title, you should treat it with suspicion and contact the ICT Helpdesk (01243 534636).
* Whilst respecting users privacy, the Council monitors and audits the use of email and IM to ensure adherence to this policy. See section 6.5
* Where GCSx email is available to connect the **sender and receiver** of the email message, this **must be used** for all external email use and must be used for OFFICIAL-SENSITIVE material.
* Automatic forwarding of email is not permitted to prevent or OFFICIAL-SENSITIVE material being forwarded inappropriately.
* In the event of prolonged absence, your line manager may need to request ICT to access your email to continue the business operations.

## Internet Acceptable Usage Policy

Policy Statement

Chichester District Council will ensure all users of Council provided internet facilities are aware of the acceptable use of such facilities.

Key Messages

* You must familiarise yourself with this policy, before using the internet facility provided. Internet and email access is an important aide to productivity.
* Private Internet and e-mail usage must be in personal time, or as per manager’s discretion.
* You are responsible for ensuring the security of their Internet account logon-id and password.
* Do not disclose your password or share accounts with colleagues.
* Individual user log-on id and passwords must only be used by that individual user, and they must be the only person who accesses their Internet account.
* Corporate Wi-Fi is NOT for personal devices
* Visitors to EPH on Council business, who require access to the internet, can be provided with Wi-Fi access under supervision of a member of CDC staff or by contacting the ICT Service Desk.
	+ Partner access Wi-Fi provides access to the Internet only and not the Council’s corporate network. The password code for the Partner Wi-Fi changes on the first Monday of each month and is available on the intranet or by contacting the ICT Service Desk.
* You **must not** create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive. If you inadvertently access an inappropriate site, immediately notify the ICT Service Desk (Ext. 01243 5(34636)).
* Certain websites are blocked, using a filtering system, see section 6.5 in the policy
* You must assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.

## Software Policy

Policy Statement

Chichester District Council will ensure the acceptable use of software by all users of the Council’s computer equipment or Information Systems.

Key Messages

* All software acquired must be purchased and installed by the ICT Service.
* Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
* Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.
* Laptops must be connected to the corporate network directly every 28 days, not via the VPN, to enable updates to be made i.e. Windows patches and Antivirus
* Unauthorised changes to software **must not** be made.
* Users are not permitted to bring software from home (or any other external source) and load it onto Council equipment.
* No user may install any free or evaluation software onto the Council’s systems
* Users **must not** attempt to disable or reconfigure the Personal Firewall software.
* Illegal reproduction of software is subject to civil damages and criminal penalties.

## IT Access Policy

Policy Statement

Chichester District Council will establish specific requirements for protecting information and information systems against unauthorised access.

Chichester District Council will effectively communicate the need for information and information system access control.

Key Messages

* All users must use **strong** passwords,
* At least twelve characters
* Contain a mix of alpha and numeric, with at least one digit, one upper case letter, one special character – not the £ sign
* Passwords must be protected at all times
* Never reveal your passwords to anyone.
* Never use the 'remember password' function
* If you write your passwords down or store make sure no one else can see them
* Never store your passwords in a computer system without encryption.
* Do not use any part of your username within the password
* Do not use the same password for systems inside and outside of work
* If you suspect your account has been compromised please inform ICT
* User access rights should be reviewed at regular intervals
* If you leave your desk, lock or log out from your terminal. The easiest way to do this is by pressing the Windows Logo key and ‘L’
* It is a user’s responsibility to prevent their userID and password being used to gain unauthorised access to Council systems
* Informing the ICT Service Desk of any changes to their role and access requirements in accordance with their manager
* Partner agencies or 3rd party suppliers must not be given details of how to access the Council’s network without permission from ICT Operations
* Partners or 3rd party suppliers must contact the ICT Service Desk before connecting to the Chichester District Council network

## GCSx Acceptable Usage Policy and Personal Commitment Statement

Policy Statement

It is Chichester District Council policy that all users of GCSx understand and comply with corporate commitments and information security measures associated with GCSx. Some Council staff will be required to have access to the facilities operated on this network in order for them to carry out their business. This may include staff having access to a secure email facility. All staff requiring access to the GCSx network in any way will be required to read and understand this Acceptable Usage Policy (AUP) and sign the Personal Commitment Statement.

This policy and statement does not replace the Council’s existing acceptable usage, or any other, policies. It is a supplement to them.

Key Messages

* Each GCSx user must read, understand and sign to verify they have read and accepted the policy.

## Human Resources Information Security Standards

Policy Statement

Line Managers will ensure that individuals are checked to ensure that they are authorised to access Council information systems.

Line Managers and ICT will ensure that users are trained to use information systems securely.

Line Managers and ICT Operations will ensure that users are promptly removed from systems when the requirement for access ends.

Key messages

* The induction process will define users responsibilities for information security and ensure users are aware of, and understand, the following policies:
	+ Information Protection Policy.
	+ Email Policy.
	+ Internet Acceptable Usage Policy.
	+ Software Policy.
	+ GCSx Acceptable Usage Policy and Personal Commitment Statement.
	+ IT Access Policy.
	+ Information Security Incident Management Policy.
* Background verification checks must be carried out on all users.
* Users who require access to “OFFICIAL - PROTECT” or “OFFICIAL - SENSITIVE” information and / or require use of the Government Connect Secure Extranet (GCSx) email facility **must** be cleared to “Baseline Personnel Security Standard”.
* All users must receive appropriate information security, awareness training and regular updates in related statute and organisational policies and procedures as relevant for their role.
* Processes must be implemented to ensure that all access rights of users of Council information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.
* All users will receive appropriate training and regular updates in legislation and procedures.

## Information Protection Policy

Policy Statement

Chichester District Council will ensure the protection of all information within the custody of the Council.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Key Messages

* The Council must draw up and maintain inventories of all important information assets.
* All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF).
* Information up to SECRET sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance.
* Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
* Users should not be allowed to access information until Line Manager and/or Personnel. are satisfied that they understand and agree the legislated responsibilities for the information that they will be handling, and are aware of any data that is regarded OFFICIAL - PROTECT and OFFICIAL – SENSITIVE
* It is a disciplinary offence to access and/or process CDC personal data for any purpose
other than in the administration required by official duties
* OFFICIAL - PROTECT and OFFICIAL – SENSITIVE information **must not** be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
* Disclosing OFFICIAL - PROTECT and OFFICIAL – SENSITIVE classified information to any external organisation is **prohibited**, unless via the GCSx email or encrypted email.
* Where GCSx email is available to connect the sender and receiver of the email message, this **must be used** for all external email use and must be used for communicating OFFICIAL - PROTECT and OFFICIAL – SENSITIVE material.
* Information is to be handled in accordance with the Disposal Policy and destroyed appropriately
* Where information is shared or disclosed, it should only be done so in accordance with the Council’s Data Sharing Policy.

## Computer, Telephone and Desk Use Policy

Policy Statement

Chichester District Council will ensure that every user is aware of, and understands, the acceptable use of Chichester District Council’s computer and telephony resources and the need to operate within a “clear desk” environment.

Key Messages

* When you are driving on council business, you must not answer a mobile phone, whether or
not it is a hands-free set. Safely park the vehicle and turn off the engine before you answer
or return the call. This also applies when you are driving any other Council vehicle e.g.
between work and home.
* Users must maintain a clear desk
* When away from your machine, whatever the location, use the windows key and ‘L’ to lock it
* Chichester District Council “OFFICIAL - Protect” or “OFFICIAL - SENSITIVE” information must be stored in a facility (e.g. lockable safe or cabinet) commensurate with this classification level.
* Do not leave anything on or near the MFD
* Users are responsible for the physical security of the device, for example keep out of sight when travelling
* Users must adhere to Chichester District Council Telephone Acceptable Use Policy / Code of Practice at all times.
* Private telephone calls should be made as per managers discretion
* No payment is required for telephone calls but phone use is audited and any abuse will be considered a disciplinary issue.
* Users handling restricted data must maintain a clear desk at all times.
* ICT equipment is provided for use on official business only.
* Do not use CDC equipment to access personal web based email
* Personal mobile phones should be switched to silent during business hours.

## Legal Responsibilities Policy

Policy Statement

This policy sets out the responsibilities of all staff under the Data Protection Act 2018 and Freedom of Information Act 2005 and other relevant legislation.

Key Messages

* Personal data is data that relates to a living individual who can be identified.
* Individuals have the right to request access to their personal information held either in paper or electronic copy by the Council. The Council has 20 calendar days in which to supply this information.
* The Council will ensure compliance with the Data Protection Act 1998 and the Data Protection Act 2018.
* The Council has established a number of roles to assure compliance of this policy.
* Every Council user has a duty to provide advice and assistance to anyone requesting information under the Freedom of Information Act.
* All councillors must accept responsibility for maintaining Information Security standards within the Council.
* If you receive a request for information under the Data Protection Act 1998, and/or Data Protection Act 2018, you should refer this request to the Council’s Data Protection Officer.
* The Freedom of Information Act 2005 allows access to records held by public authorities. If you receive a request for information under the Freedom of Information Act 2005 The Freedom of Information Act 2005 allows access to records held by public authorities. A request will come through the contact centre who will distribute to the correct department. Once this has been completed a copy will be sent back to the contact centre and if appropriate Public Relations
* It is a disciplinary offence to access and or process personal data for any purpose other than in the administration required by official duties
* Line managers must ensure that all staff receive ‘display screen equipment ‘(DSE) assessment to ensure their staff are working within a safe and healthy environment. There are qualified staff in each service area who will be able to understate these assessments for you. If you are unsure to they are, contact the Health and Safety Team

## Remote Working Policy

Policy Statement

Chichester District Council provides users with the facilities and opportunities to work remotely as approved by the Director or Head of Service. Chichester District Council will ensure that all users who work remotely are aware of the acceptable use of portable computer devices and remote working opportunities. Portable computer devices include:-

* + Laptops/tablets
	+ Mobile Phones
	+ Access Tokens
	+ Wireless technologies

Key Messages

* When working remotely staff will use corporate laptops.
* All ICT equipment supplied to users is the property of Chichester District Council. When required by ICT Service access must be given to allow essential maintenance security work or removal.
* Seek advice from the ICT section if you need to take equipment outside of the United Kingdom as it will not be covered by the Council’s insurance.
* Users must not access GCSx type services, facilities or OFFICIAL-SENSITIVE information on personal equipment
* Users must take due care and attention of portable computer devices when travelling when not in use lock it out of sight
* Users must not install, attempt to install or update any software on corporate devices
* Users must not add any hardware to or inside any council owned portable computer device
* Users must inform the ICT Service Desk of any error message(s) or faults
* Data should NOT be stored on portable computer devices, if there is a business need for the information to be available on the local device (laptop) please contact the ICT Service Desk for advice
* Limited personal use is allowed as long it is not related to running a business
* Users must follow policy for accessing sites as if at work
* Staff members must not use CDC kit to access personal email
* Staff members must not allow third parties to use the device i.e. family members
* Users must not send Council information or documents to a private email address at home to work on
* Do not email OFFICIAL-SENSITIVE or above information to a non-Council email address unless encrypted
* Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location. Both personal and data.
* Portable computer devices should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes
* Use Outlook to inform colleagues when working remotely with times blocked out as unavailable, when not working.
* It is the user’s responsibility to ensure that access to all OFFICIAL- SENSITIVE or above information is controlled
* OFFICIAL-SENSITIVE or above data must not be held on portable computer devices
* Access to information classified as OFFICIAL-SENSITIVE or above MUST be via equipment provided by the Council.
* If you need to take paper confidential or sensitive information off-site, you must get authorisation from your Line manager. This should be avoided where at all possible.
* Access tokens should be kept separate from the device, as you would never keep your bank card and PIN together
* Laptops should regularly connect directly to the network in a site office – for example EPH to enable updates

## Removable Media Policy

Policy Statement

Chichester District Council will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems and IT equipment for the purposes of conducting official Council business.

Key Messages

Removable media devices include:-

* Memory stick/USB Keys
* CDs
* DVD
* Laptop
* Camera
* Memory Cards
* Floppy Disks
* iPads
* Optical Disks
* External Hard Drives
* Media Card Readers
* Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
* MP3 Players
* Backup Cassettes
* Audio Tapes (including Dictaphones and Answering Machines)
* It is Chichester District Council policy to limit the use of removable media devices. The use of removable media devices will only be approved if there is a valid business case for its use.
* Any removable media device that has not been supplied by IT **must not** be used.
* All data stored on removable media devices **must** be assessed and encrypted when required.
* Damaged or faulty removable media devices must not be used.
* If you receive a CD or memory stick from a third party, you must take it to the ICT Service Desk who will check that it has no viruses on it before you insert it into your laptop or P.C. They will return it to you with a label certifying that it is virus-free. Always check that any device has this label on it before using it.
* Removable media devices that are no longer required, or have become damaged, must be returned to ICT Operations to dispose securely and avoid data leakage.
* If you suspect there has been a breach please follow the Information Security Incident Management Policy and contact the ICT Service Desk immediately on 01243 5(34636).

## Information Security Incident Management Policy and Procedure

Policy Statement

Chichester District Council will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the Council.

Key Messages

* All staff must report any incidents or suspected incidents immediately by contacting the ICT Service Desk and Line Manager.
* If you are unsure of anything in this policy you should ask for advice from the DPO

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

**Malicious**

* Giving information to someone who should not have access to it - verbally, in writing or electronically.
* Computer infected by a Virus or other malware.
* Sending a sensitive e-mail to 'all staff'
* Receiving unsolicited mail of an offensive nature.
* Receiving unsolicited mail which requires you to enter personal data.
* Finding data that has been changed by an unauthorised person.
* Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
* Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

**Misuse**

* Attempting load, remove or reconfigure any software, or change the settings on any system, provided for the council’s use without the permission of, or under guidance from, ICT.
* Connecting, or attempting to connect, any device to the council’s ICT infrastructure without the permission of ICT. This may include connecting, computers and other devices (such as mobile phones, digital cameras, music players etc.) by which data can be transferred directly to the network or another computer either through a wired or wireless connection.
* Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password).
* Writing down your password and leaving it on display / somewhere easy to find.
* Printing or copying confidential information and not storing it correctly or confidentially.

**Theft / Loss**

* Theft / loss of a hard copy file.
* Theft / loss of any Chichester District Council computer equipment.
* Theft/loss of disposable media.

## Communications and Operation Management Policy

Policy Statement

Chichester District Council will ensure the protection of the Council IT service (including any information systems and information processing equipment used by the Council) against malware and malicious and mobile code.

Only authorised changes will be made to the Council IT service (including any information systems and information processing equipment).

Information leakage will be prevented by secure controls.

Key Messages

* Any changes to a system, e.g. an upgrade, patch or additional software must be referred to ICT via a formal change request.
* Unpatchable software must not be used where there is GCSx connection provided.
* Appropriate access controls are put in place to prevent user installation of software and to protect against malicious and mobile code.
* Regular backups of essential business information are taken to ensure that the Council can recover from a disaster, media failure or error.
* If you need to dispose of a CD or other form of media, contact the ICT Service Desk who will arrange for its safe disposal.
* System audit logs for RESTRICTED data and GCSx services must be kept for a minimum of six months.
* Connections to the Council network are made in a controlled manner.
* An annual health check must be made of all Council IT infrastructure to maintain security.

## IT Infrastructure Security Policy

Policy Statement

There shall be no unauthorised access to either physical or electronic information within the custody of the Council.

Protection shall be afforded to:

* Sensitive paper records.
* IT equipment used to access electronic data.
* IT equipment used to access the Council network.

Key Messages

* Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A Council ICT employee must monitor all visitors accessing secure ICT areas at all times.
* OFFICIAL - PROTECT and OFFICIAL – SENSITIVE information, and equipment used to store and process this information, must be stored securely.
* Non-electronic information must have appropriate information security controls in place to protect it.
* Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by ICT Operations, as appropriate. Keys are not stored near these secure areas or lockable cabinets.
* Do not loan your ID badge, keys, entry codes or access tokens to anyone else.
* Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge.
* A Council ICT employee must monitor all visitors accessing secure ICT areas at all times.
* All general computer equipment must be located in suitable physical locations to limit the threat of theft or data loss
* Desktop PCs or laptops should not have data stored on the local hard drive.
* All items of equipment must be recorded on the ICT Service inventory
* Non-electronic information must be assigned an owner and a classification. OFFICIAL information must have appropriate information security controls in place to protect it.
* Shut down laptops when transported so device encryption is enabled
* When taking equipment out of the office be aware of the physical security dangers and risks associated with working within any remote office or mobile working location. Both personal and data
* Staff should be aware of their responsibilities in regard to the Date Protection Act
* Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed by the ICT Service

## Bring Your Own Device (BYOD) Policy

Policy Statement

Chichester District Council will ensure all users of the Council who use a Bring Your own Device (BYOD) are aware of the acceptable use of this facility.

Key Messages

* Any request for BYOD must be in writing (TrackIT) and agreed by your manager
* All devices must be encrypted
* The Mobile Device Management (MDM) application provides separation between corporate data and personal data
* It is an application to provide access to email and calendar
* In addition the facility to access Disaster Recovery Documents may also be available
* CDC do not have access to your personal information on your BYOD, however if satellite navigation is enabled we may track your device, if requested.
* Users MUST inform ICT if their device is lost, stolen or otherwise compromised so that the data within MDM application can be remotely wiped
* The MDM or MiCollab applications cannot be installed on jail broken devices
* Alerts must be disabled so email headers cannot be seen without domain password
* The device must be secured by a pin or biometric finger print
* ICT Service desk will ONLY support the MDM application on your device. We will not change ANY settings on your device
	+ If there is a problem the extent of our support is to uninstall and then reinstall the MDM or MiCollab application
* Agreeing to have this application on your device is entirely at your own risk
* Business calls made through MiCollab when your phone is connected to Wi-Fi will not be charged
* Costs of business related phone calls out side of MiCollab are NOT included in this policy therefore; business calls will need to be accounted for separately*.*
* Data costs will not be reimbursed.
* CDC has a zero-tolerance policy for calling, texting or emailing while driving
* You must not use a mobile phone (even with hands-free) whilst you are driving at work.
* When a user leaves they must inform ICT so the MDM application can be removed from the BYOD device
* Use of BYOD and the MDM application is a privilege and will be taken away if misused
* There is a cost associated to this service therefore authorisation is required from the budget holder.
* Use of the MDM application to access emails and calendars and/or MiCollab application out of office hours, is at the discretion of the user

# Policy Compliance

If any user is found to have breached this policy, they may be subject to Chichester District Council’s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the DPO.

# Policy Governance

The following table identifies who within Chichester District Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

* **Responsible** – the person(s) responsible for developing and implementing the policy.
* **Accountable** – the person who has ultimate accountability and authority for the policy.
* **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
* **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

|  |  |
| --- | --- |
| **Responsible** | Director of Corporate Services, Divisional Manager Business Support, DPO, ICT Manager  |
| **Accountable** | Section 151 Officer, SIRO, DPO  |
| **Consulted** | Corporate Policy and Performance Management, Human Resources, Joint Employee Consultation Pane, CMT, Corporate Governance & Audit Committee |
| **Informed** | All Council Employees, All Temporary Staff, All Contractors, Members |

# Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Divisional Manager Business Support

# References

This Policy must be read in conjunction with the following supporting documentation:

* Email Policy
* Internet Acceptable Usage Policy
* Software Policy
* IT Access Policy
* GCSx Acceptable Usage Policy and Personal Commitment Statement
* Human Resources Information Security Standards
* Information Protection Policy
* Computer, Telephone and Desk Use Policy
* Legal Responsibilities Policy
* Remote Working Policy
* Removable Media Policy
* Information Security Incident Management Policy
* Communications and Operation Management Policy
* IT Infrastructure Policy
* Data Sharing Policy
* Data Quality Policy
* Data Protection Policy

# Personal Commitment Statement

|  |  |
| --- | --- |
| Name of User: |  |
| Position: |  |
| Department: |  |

I accept that I have been granted the access rights to Chichester District Council systems and data. I understand and accept the rights, which have been granted, I understand the business reasons for these access rights, and I understand that breach of them, and specifically any attempt to access services or assets that I am not authorised to access, may lead to disciplinary action and specific sanctions. I also accept and will abide by this policy, personal commitment statement. I understand that failure to comply with this agreement, or the commission of any information security breaches, may lead to the invocation of the Council’s disciplinary policy.

Signature of User: ……………………………………Date: …………….. Document Version: V2.6

A copy of this agreement is to be retained by the User and Personnel Department.