DDaT IT Security Policy

Date created:	April 2022
Current version:	1.1
Author:	Kate Waterhouse – Chief Information Officer
Owner:	Richard Rothwell – Cyber Security & Compliance Officer
Verified by:	Information Governance Steering Group
Date of Approval:	January 2025
Review date:	January 2025
Update history:	1.0 – document created 1.1 – document reviewed and changes made to update
Document type:	IT Security Policy
Classification:	Supporting Documentation

Contents

Glossary of Acronyms

DDaT	Digital Data and Technology
IT	Information Technology
GDPR	General Data Protection Regulation
UK	United Kingdom
MCT	Malicious Call Tracing
VPN	Virtual Private Network
CMS	Content Management System
HR	Human Resources
UPS	Uninterrupted Power Supply
CD	Compact Disc
DVD	Digital Versatile Disc

1 Introduction

This policy has been developed to ensure all IT systems used at Bury Council are developed, operated and maintained in a safe and secure manner. This has been increasing relevant as modern technology is introduced and everyone embraces new ways of working.

The Council's IT Security Policy **applies to all its elected members, employees, agents and contractors,** who directly or indirectly support, or have, access to Council Information Systems.

All elected members, employees, agents, and contractors are responsible for ensuring the security of the equipment and systems they use, whether on Council premises or any other location, as part of the Council's agile working approach.

The Council's IT Security Policy applies to all departments of the Council. No other departmental policies or variations from the corporate policy are permitted. If departments feel that the corporate policy does not cover all their requirements, they must contact the DDaT Service Desk in the first instance.

1.1 Aims and Objectives of the Council's IT Security Policy

The main aims of this policy are:

- To ensure that IT systems used within Bury Council are assessed for appropriate levels of security to maintain the confidentiality, integrity and availability of information and information systems.
- To ensure that all the Council's IT assets; people, software, information and hardware equipment are adequately protected, against threats to the level of IT service required by the Council.
- To ensure that elected members, employees, agents and contractors are aware of and fully comply with all UK legislation.
- To create, across the Council, a level of awareness of the need for IT Security to be an integral part of the day-to-day operation of the Council's systems.

1.2 Personal Commitment Statement

All elected members, employees, agents and contractors who need to use the Council's network are required to sign up to the Council's current Personal Commitment Statement (Appendix A).

All new starters are required to successfully complete the Council's UK GDPR training suite (online module or paper-based for staff without access to computer systems) within the first five days of their employment as a condition of being given network access.

All existing elected members, employees, agents and contractors are required to repeat and pass this training on an annual basis.

If this training is not done in five days of starting or not repeated after 12 months access will be withdrawn at request of Data Protection Officer until the matter is resolved.

2 Responsibilities

All elected members, employees, agents and contractors are responsible for the confidentiality, security and accuracy of Bury's IT facilities, irrespective of the location where they are working.

Failure to comply with the provisions of this policy or related documents may lead to disciplinary action and/or criminal proceedings.

2.1 On-going management of the security policy

The IT Security Policy is maintained by the DDaT unit on behalf of the Information Governance Steering Group and will be subject to regular review (at least every two years or immediately on introduction of new related legislation) to ensure that it remains both relevant and up to date.

2.2 Access to the Council's network

2.2.1 Standard Access

All staff working for the Council are provided with access to the Council's network so that they can use a computer to access Council systems, including email.

New employees will be provided with a username and initial password for connecting to the network and will be issued with a Welcome Pack from the DDaT Service Desk. This pack includes a **Personal Commitment Statement** (Appendix A) which they must read and agree to have ongoing access to network facilities.

Managers of new employees will be reminded in the induction pack that the new starter must also complete the mandatory UK GDPR training within five working days of joining the Council, otherwise their network access will be revoked. If access is revoked, this will only be reinstated after a completion date is agreed with the Information Governance manager.

Similarly, all staff must repeat and pass the Council's UK GDPR training module on an annual basis. Any member of staff failing to do this after reminders being sent will also have their IT access withdrawn. This will only be reinstated when a training completion date is agreed with the Information Governance manager.

2.2.2 Agile Working

The Council provides network access gateways for staff to work remotely in line with the Council's Agile Working Policy

3 System Security

3.1 Access Control

Each user will be allocated access rights and permissions to computer systems and data commensurate with the tasks they are expected to perform.

If you require access to the Council's computer systems, you must firstly contact your line manager for authorisation. The line manager must then process the request via the DDaT Service Desk.

3.2 User Password Management

Access to the Council's computer network must be dependent upon the entry of a valid Userid and Password.

- Each user **must** have their own Userid and password.
- All users **must** have unique passwords for both connecting to the network and for access into different systems.

The DDaT unit ensures that network passwords are set to expire automatically after 90 days, and the user is asked on screen to change their password.

Where it is not possible to enforce automatic password changes on individual systems, the system owner should set standards for password changes, and devise procedures to ensure compliance.

Where computer systems or files are to be password protected, line managers responsible for the systems must ensure that suitable procedures are in place to control password use.

- Passwords **must** be a minimum of fourteen (14) characters and be based on 3 Words or a phrase. This creates a more memorable, longer and stronger password. The password needs to consist of a mixture of upper- and lower-case letters and/or numbers/symbols. You must avoid the use of passwords based on names of family members and pets, car registration numbers and simple patterns of letters from a computer keyboard. Please note, that you should **never use** any derivation of the word 'password' as your password.
- Passwords **must never** be disclosed to anyone. Keep your password secure and private.
- The use of another person's Userid and Password is not allowed.
- Temporary passwords **must** be changed at the first sign on.
- Passwords **must not** be written down.
- Passwords **must** be changed immediately if it is suspected or known that it has been compromised, and the matter reported to the DDaT Service desk. The compromised password **must** never be used partly or in full for any future password.
- Passwords **must not** be included in any automated sign on procedures, macros or function keys.
- **Do not** use the same or similar password for your Council work password that you use for personal accounts. Keep personal and Council work passwords totally separate.

3.3 User Responsibilities

Employees must not examine, change or use another person's email account, files, or output for which they do not have explicit authorisation.

Computers must not be left unattended when signed on. Whenever you leave your computer, you **must** lock the screen (press the Windows key and L) to prevent anyone using it in your absence. This is to protect Council data and the integrity of your own email facilities. If any computers are left unattended inadvertently (and/or are unused), then the screen will lock automatically after 20 minutes.

All users must sign out of all systems when you have completed your work shift and switch off any computer unless specifically requested not to do so.

In addition to security considerations, this saves electricity and reduces the risk of fire.

3.4 Public Access Computers

Where computers are provided for public access, consideration must be given to computer system security and the security of the Council's network and other computer networks. This can be achieved through the implementation of specialist software and an Acceptable Use policy.

Contact the DDaT Service Desk for advice and guidance on specialist software that helps to maintain system security on public access computers.

3.5 Revoking Access

When an employee leaves the Council, their access to computer systems and data must be revoked on conclusion of the employee's last working day. It is the responsibility of the line manager within each directorate to request access is revoked via the DDaT Service Desk.

Similarly, the new employee's line manager must inform the DDaT Service Desk when any staff changes job title and/or becomes a new member of their team within the Council. This request must be submitted by email or via the Self-Service portal to the DDaT Service Desk to amend that user's identifiable details and systems access as appropriate.

3.6 Use of personal phones or devices for accessing Council systems.

It is recognised that employees on occasions, use their own electronic devices for Council business particularly their Council email account. Employees who use their personal device must complete a Personal Device Agreement which can be obtained from the DDaT Service Desk. The salient points from that agreement are as follows:

- The Council has the right to delete its data from the device or lock the device or that data.
- The Council has the right to scrutinise the device.
- The employee will allow the device to be physically inspected.
- Access to the device will be protected using a strong password or passcode and, where possible, the device will be encrypted.
- The employee will not download documents containing personal data or other material to the device.
- The employee will regularly check the device to ensure that no files have been accidentally downloaded and stored on the device (e.g. by accidentally downloading an attachment to an email). Any such file found needs to be deleted immediately.
- The employee will check the device before allowing someone else to use it
- Before disposing of the device, the employee will ensure that all Council data has been removed from the device.
- The employee understands their responsibility for safeguarding all Council data.
- The employee will inform DDaT Service Desk immediately if the device is lost or stolen.
- The employee understands that if they do not comply with or break the personal device agreement, then they may be subject to disciplinary action.

4 Data Security

All Council data remains the property of the Council and is confidential. All employees must take due care when handling and sharing Council data to prevent unauthorised access to information; this applies to all information, whether it is held on a computer or on any other media, including paper.

4.1 Line Managers Responsibilities

Line managers are responsible for agreeing and monitoring procedures for ensuring the security of work, information, data and files under an employee's control. Where individuals work in an agile way or need to work from home/out of the office, you must consider the option of Remote Access to IT Systems, which provides secure access to IT systems and files. Contact the DDaT Service Desk to arrange this.

Line managers must take due care in the positioning of computer monitors in public areas, taking into consideration the sensitivity of the information that may be displayed on them.

4.2 Users Responsibilities

Whether working at a Council location or at another site, including the employee's home; employees must take all reasonable precautions to protect information relating to employment with the Council.

There is no case, given the Council's use of cloud-based data storage within Microsoft Teams, OneDrive and SharePoint along with Remote Access, for computer files to be held on removable media such as pen drives.

These security principles also apply to more traditional tools, such as paper.

It is recommended that agile working employees keep work life and domestic life separate. Where there is a risk that other household occupants might gain sight and/or access to work related computer files, you must position your computer and screen so that only you can have access. Lock your computer when absent.

Care must be taken not to inadvertently disclose passwords. Passwords must never be shared with anyone.

Employees must comply with the Council's systems and departmental procedures for keeping their computer or mobile device up to date for any software or security updates by restarting the computer or smartphone when prompted and convenient to do so.

Also locking the computer or smartphone; signing off the computer or if applicable shutting down the computer when it is not in use.

5 Telephony

All requests for telephone installations or changes to telephone details must be made to the DDaT Service Desk.

Telephone numbers used in email signatures must be either the Council's main contact number or, where available, an officer's direct line or work mobile number. Under no circumstances must personal mobile or landline numbers be used.

5.1 Mobile Phones

Should you require a mobile phone for Council work purposes, you must contact your line manager, in accordance with departmental procedures. All new mobile phones must be obtained in line with corporate arrangements through Corporate Procurement. Mobile phones provided by the Council must be used in accordance with the current Mobile Telephone User Procedure.

5.2 Telephone Bills

All telephone lines should form part of the Council's corporate contract. All invoices for telephone usage and rental are paid centrally and are monitored and checked by the DDaT unit's Telephone Team to ensure appropriate usage. If there are telephone lines which are not part of the corporate contract, then users should contact the DDaT Telephones Team to get the lines ported to the corporate contract.

5.3 Telecommunications Records and Reports

All telecommunications records and reports must be treated as confidential and disposed of as confidential waste.

5.4 SMS Texting Service

SMS texting is another mode of communication that enables users to send texts to other mobile phones and landlines. You must not use this service in any way that conflicts with email or telephone acceptable usage. Failure to comply with these provisions may result in disciplinary action.

Use of the Council's SMS texting service is subject to regular monitoring for security and/or network management reasons.

5.5 International Calls

All requests to make international telephone calls must be made to the DDaT Service Desk confirming the call is for business use and has been approved by your line manager.

5.6 Malicious Call Tracing (MCT)

MCT is a call recording system for use when dealing with an abusive or threatening caller. This must only be used in very serious cases e.g. where the caller is threatening the safety of the staff member, other staff members, the Council or the Public. If you require this facility, your line manager should contact the DDaT Service Desk.

6 Internet and Intranet web site development

The Council manages its external websites and Intranet through a Content Management System (CMS). Under this system, responsibility for the content of web pages for one or more service areas is devolved to the appropriate "editors". Each service area may also have an "approver" otherwise known as a moderator to check and authorise any changes made to web pages by the editors. There is a pool of trained web editors who are responsible for the editing and moderating all the web pages for all service areas in that department.

Other website and web systems e.g., Libraries' Web catalogues, should be approved by the DDaT management team and follow the corporate style and accessibility standards.

6.1 Internet Access and Use

The DDaT Service Desk must approve all requests for Internet access.

Use of the Internet is permitted and encouraged where such use is suitable for Council business purposes. Access to the Internet on the Council's equipment is permitted for personal use in non-working time.

Users of the Internet should be aware that all Internet activity is continuously monitored and recorded. The Council reserves the right to monitor all usage in accordance with the Human Rights Act 1998 and Regulation of Investigatory Powers Act 2000.

Use of the Council's equipment for personal access to the Internet is made entirely at an individual's own risk.

6.1.1 Misuse of Internet Access

The Council's Internet facilities must not be knowingly and deliberately used to access or download the following types of information:

- Criminal information (e.g. racist or terrorist propaganda).
- Pornography, abusive, defamatory, offensive, obscene or malicious information.
- Information that makes improper or discriminatory reference to e.g. but not exclusively to the following: a person's ethnicity, religion or belief, gender, gender re-assignment, sexuality, sex life, philosophical beliefs, trade union memberships, age, national origin, disability, caring responsibilities or physique.
- Any information that might be perceived as damaging or likely to damage the Council's reputation.

To access any filtered sites in accordance with the duties of employment, permission must be obtained from a line manager with an email request sent to the DDaT Service Desk.

Anyone encountering inappropriate websites or information by accident, must inform the DDaT Service Desk. The DDaT Infrastructure & Cloud team must also ensure that the website is added to the Council's Internet Firewall to prevent further access.

Elected members, employees, agents and contractors **must not**:

- Use the Council's Internet facilities to upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the Council, or to the Council itself.
- Make unauthorised use of the Council's corporate logo or name on any websites.
- Use the Internet or your Bury Council email address at any time for either personal commercial purposes or financial gain, e.g. gambling/trading sites.
- Download software or files for personal use (including video, music, other multimedia, etc.) using "peer to peer networking" or similar technologies even during your own time.
- Send via email, Council data or files of any kind, especially those that are confidential, personal or business sensitive either to or from your own personal email address.

Any elected member, employee, agent or contractor found to be in breach or in any way contravening the provisions of this section will be subject to relevant disciplinary action.

6.1.2 Purchases over the Internet

You can make purchases over the Internet on behalf of the Council as long as your director has approved this for your department.

You may make personal purchases on the Internet in your own time, at your own expense and entirely at your own risk; providing that the goods are not delivered to Council premises, and you do not provide in any part of that transaction, a Council email address or telephone number.

6.1.3 Public Internet use in Council libraries

Council libraries provide public access computers, including free Internet access, to the public in Council libraries. All users of this service are subject to the libraries' Acceptable Use Policy (Appendix B).

7 Email

Any communications and information transmitted, received or archived by Bury Council computer systems, belong to Bury Council. Emails held on Council computers and email systems are part of the corporate record. Reasonable personal use is permitted, provided that it is legal, not excessive and does not interfere with work-related performance. The Council reserves the right to monitor usage of email to ensure security and operational availability. It also reserves the right to access and disclose any email to ensure compliance with all relevant UK legislation and guidance, and any other relevant policy of this Council.

7.1 Legal Implications

It should be noted that the contents of emails sent to and from the Council's email may be disclosed under the Freedom of Information Act 2000 and/or the UK GDPR and the Data Protection Act 2018. With this in mind, emails **must** be worded appropriately and **not** contain references which could be construed as:

- Insulting personally to a third party.
- A show of personal bias by an employee against someone/organisation.
- Exchange of views about the personality of a third party.

Employees must be conscious that binding contracts can be formed by the exchange of emails.

As any outgoing email will identify the sender as working for Bury Council, it may be seen as an official response. No unauthorised indication of ostensible authority to enter into contracts on behalf of the Council should be given in any email.

7.2 Monitoring Email Use

Use of the Council's email system is subject to regular monitoring and filtering for security and/or network management reasons. As such, the Council reserve the right to intercept emails that contravene the provisions of this policy, including receipt of emails containing attachments for non-business use.

You should have no expectation of privacy for any personal email that you send or receive via your work email account.

Line managers or authorised officers may access an employee's email account without the employee's permission in exceptional circumstances, such as:

- Absence (e.g. due to sickness, holiday or business commitment) where there is a need to access messages to conduct the normal functions of the Council.
- Where there is a suspicion of misuse.

7.3 Misuse of Council Email Accounts

Email has the same legal standing as other forms of written communication and requires considerable care.

You must be aware that you and/or the Council might be held liable in law for any email sent by you that could be construed as libellous or defamatory, or in connection with any fraudulent activity or criminal behaviour. It is your responsibility to ensure that your emails cannot be construed in this way. If you are unsure of the suitability of the content of an email, you should seek clarification from your line manager.

Certain types of misuse of the email system could lead to disciplinary action under the Council's existing policies e.g. the data breach and/or dignity at work policies, the staff Code of Conduct or any such established policies that may apply.

All email users must comply with the provisions of this policy; failure to do so may lead to disciplinary action.

If you receive an email that you feel is inappropriate, you must report it to your line manager and the DDaT Service Desk.

7.4 Viruses via the Email system

The Email system is protected, as far as possible, against viruses, by means of anti-virus software, which operates automatically. All users should, however, remain aware of the danger of spreading viruses. Negligent virus transmission is classed as inappropriate use of email and may be subject to disciplinary action.

The deliberate act of spreading viruses is subject to prosecution under the Computer Misuse Act 1990.

File attachments in unsolicited emails from sources that are not known or reputable **must not** be opened. Similarly, **do not** attempt to access any web links that are included in any unsolicited emails or follow any instructions that tell you to reply with personal or work information, bank details or to delete or otherwise tamper with files. Contact the DDaT Service Desk immediately if any concerns and queries.

7.5 Sending Confidential Information

When you need to send confidential information in an email message, always use 365 encryption directly and easily from Outlook. Encrypting an email message in Outlook means it is converted from readable plain text into scrambled cipher text. Only the recipient can decipher the message for reading.

For file attachments that contain confidential information, it is possible to increase the security of that information sent by email by placing it in a 'zip' file and password-protecting the zip file. The password can then be passed to the recipient by phone.

Another option is to upload the file to your OneDrive or if already on SharePoint, then share the file with the recipient's email address. Set the read or edit permission accordingly and then send them the web link to the file. The file remains within our Cloud storage and only the recipient with that email address can access the file. Later on, access to that file can be removed if required or an expiration date set and the original web link to the file will not work.

Make sure that you have sent data to the correct email address and check that they have received it.

It is recommended that a short delay is placed on all emails before sending. Any email sent incorrectly, either to an incorrect email address or contains wrongful information etc., will then give the sender the opportunity to amend before being resent. Please contact the DDaT Service Desk for guidance on this if required. Remember that emails sent outside the Council's email system cannot be recalled.

Even if sending an email and attachments internally, remember it may not be read in a secure environment as Council employees can remotely access their emails.

If an incorrectly addressed email message is received, the sender **must** be contacted immediately to inform them that this email has been received and that it will be deleted and also purged/cleared from 'deleted items' mailbox. If such emails contain confidential information, use must not be made of that information, nor must it be disclosed or sent to other people.

Care must be taken when replying to emails, particularly those that consist of a chain of passed-on emails. These emails may hold sensitive and/or confidential information. It is essential that all such emails are either read and all information thoroughly vetted before replying or forwarding on, or the chain should be severed, and a fresh email written.

7.6 Email Disclaimer

All bury.gov.uk external emails (i.e. emails sent outside the Council) automatically include the following disclaimer:

Why not visit our website www.bury.gov.uk

Incoming and outgoing email messages are routinely monitored for compliance with our information security policy. The information contained in this email and any files transmitted with it is for the intended recipient(s) alone. It may contain confidential information that is exempt from the disclosure under English law and may also be covered by legal, professional or other privilege. If you are not the intended recipient, you must not copy, distribute or take any action in reliance on it. If you have received this email in error, please notify us immediately by using the reply to facility on your email system. If this message is being transmitted over the Internet, be aware that it may be intercepted by third parties. As a public body, the Council may be required to disclose this email or any response to it under the Freedom of Information Act 2000 unless the information in it is covered by one of the exemptions in the Act. Electronic or fax service of documents is not accepted. New legislation governing the way we protect your personal data is now in force from the 25th of May 2018. For information on how we protect and look after your personal data and to find out more about your individual rights about personal data we hold on you, please go to our website: https://www.bury.gov.uk/privacy

8 Software Asset Management

Bury Council uses software in all aspects of its business to support the work conducted by its employees. In all instances we are required to have a licence for every piece of software used and Bury Council will not condone the use of any software that does not have a licence. It will be regarded as a disciplinary offence should any employee be found in possession of, or using, unlicensed software. This Policy details the procedures that must be followed when purchasing and installing software on Bury Council's IT equipment.

The successful operation of this Policy cannot be achieved without the wholehearted co-operation of every elected member, employee, agent and contractor. It is therefore imperative that employees and other relevant persons are aware of, and fully comply with, the Policy and other instructions derived from it.

8.1 Software Acquisition

All computer software must be purchased via the Corporate DDaT Team, in accordance with the Council's Financial Regulations and the Council's Procurement Procedures (including e-procurement).

8.2 Software Delivery

All computer software must be delivered according to the contract. Software downloads must be facilitated by the DDaT Service desk. All software must be included in departmental inventories.

8.3 Software Installation

The DDaT Service Desk must be contacted for software installations. The DDaT Service Desk will either install the software or make appropriate arrangements with another DDaT unit for them to install. Individual sections/officers will apply regular updates to approved software, where necessary.

8.4 Software Compliance and Documentation

The nominated officer must ensure that the appropriate software licence is obtained for all software purchased or installed in their department/team. Software licences and any other proof of licence must be recorded.

The DDaT Service Desk is responsible for ensuring that an inventory is maintained of all software licences purchased by Council.

8.5 Software Movements

The DDaT Service Desk must be contacted when software needs to be installed and/or deleted. The nominated officer must update software inventories accordingly.

8.6 Software Disposal

The DDaT Service Desk facilitates the removal of software and updates the software inventory.

8.7 Shareware, Freeware and Public Domain Software

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all software, no user may install any free or evaluation software onto the Council's systems without prior approval from the DDaT Service Desk.

8.8 Games and Screensavers

Only the Council's standard screensaver and Desktop wallpaper are to be used.

Games that form part of the operating system must only be used in employees' own time. Use of any other games is prohibited. Games or screensavers must not be downloaded from the Internet.

8.9 Illegal Software Copying

You must not make copies of computer software owned by Bury Council for private use. Misuse of the Council's software in this manner will result in disciplinary action.

8.10 Control of proprietary software copying

Proprietary software products are usually supplied under a licence agreement that limits the use of the products and limits the copying to back-up copies only.

In line with the Copyright, Design and Patents Act 1988, it is Council policy that no copyright material is to be copied without the owner's consent.

If copies of software in excess of those specified in the licence agreement are required, the owner's written consent must be obtained. This consent must then be held together with the licence.

Under certain licence agreements, a copy of the software may be held on computers not belonging to the organisation. Clarification of the legal position must be obtained before installing such a copy, which must then conform to all requirements of the owner.

9 Hardware Asset Management

9.1 Hardware Acquisition

All computer hardware must be purchased from the Council's approved hardware suppliers via the nominated officer, in accordance with the Council's Financial Regulations and the Council's Procurement Procedures (including e-procurement).

9.2 Insurance of IT Equipment

A three-way discussion is required between Information Governance, the Business manager and DDaT to examine whether the Council's "all risk" policy covers the risk of hardware loss, theft and damage.

9.3 Hardware Maintenance

Maintenance of IT equipment must only be undertaken by the DDaT unit, or a contractor approved by the DDaT unit. All maintenance requests and fault reporting must be made to the DDaT Service Desk.

9.4 Hardware Inventories

The DDaT unit is responsible for ensuring that all IT equipment is asset labelled and recorded in the hardware inventory. Officers must ensure that all computer hardware is included in departmental inventories, in accordance with Financial Regulations. This inventory must include a description of the equipment, the serial number and the IT asset number.

9.5 Hardware Movements

The DDaT Service Desk must be notified of all movement of hardware equipment.

No IT equipment may be removed, except by the DDaT unit, or a contractor appointed by the DDaT unit. Employees must not take offsite any equipment, data or software, without management authorisation.

The DDaT Service Desk will maintain records detailing all IT assets taken off-site, including in people's homes.

9.6 Hardware Disposal

The DDaT Service Desk must be notified and will subsequently ensure that all IT equipment is disposed of in accordance with the Council's Procedure for the disposal of computer software and IT equipment.

10 Computer Systems and Data

All computer programmes and data developed by the Council are for the sole purpose of the Council's business and access by members and employees is solely for this purpose except by express written permission of the Council, Chief Executive, or Chief Officer.

10.1 Virus Controls

Anti-virus software must be installed on all servers and networked and standalone computers. The DDaT unit is responsible for ensuring that the anti-virus software is automatically updated on all servers and networked computers.

The following procedures **must** be followed to minimise the risk of software virus infection:

- The DDaT Service Desk **must** be contacted about software installations.
- You **must** not open attached files or click on web links from unsolicited emails that do not originate from known or reputable sources. If in doubt, contact the DDaT Service Desk.
- All Council-owned computers **must** be connected to the Council network and powered on at least once a month for at least one hour in order to receive the latest operating system, anti-virus and application version updates.
- To ensure that all Smartphones are regularly updated with the latest anti-virus software and security software updates, they **must** be connected to the internet either via mobile internet or ideally Wi-Fi connection.

10.2 Procurement of Computer Systems

The provisions of this policy and the Council's Contract Procedure Rules, Financial Regulations and relevant procurement procedures must also be considered during the procurement of new computer systems.

The DDaT Service Desk must be informed of all proposals for software and hardware procurement, or software development.

10.3 Systems Development

Staff negotiating contracts, under which specific software is to be written for the Council must seek to ensure that suitable arrangements are made for the copyright to be vested in the Council.

The Council owns the Copyright for all software that has been developed by employees and contractors in the course of their employment with the Council, for specific use by the Council.

The DDaT unit's staff must have automatic access to live applications, and all amendments to executable code must comply with the DDaT unit's change control procedures.

The owner of the system and the DDaT unit must monitor all activity within live systems.

11 Computer and Network Management

You must not intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that hinders others in their use of the network.

11.1 General Housekeeping

It is vital that backup procedures are in place and documented to maintain the availability, integrity and confidentiality of data.

The DDaT unit must ensure that appropriate back-ups are undertaken for all servers located on-premises and in the cloud.

11.2 Procedures

The following procedures **must** be followed:

- all servers are backed up nightly; the schedules start after 19:00. A full backup is run every Friday evening/Saturday morning, an incremental backup is run Monday-Thursday. The full backups are retained for 4 weeks.

11.3 Desktop computers, Laptops, Tablets and all mobile devices

With the advent of Microsoft Teams, OneDrive and SharePoint, there is no case for computer files to be stored locally on the device. Such data is at risk of not being backed up as well as becoming the source of a data breach.

11.4 Network Management

If you require access to the Council network, you must contact the DDaT Service Desk. New starters will be given access from their first day of employment. However, they must complete and pass the Council's Information Governance training suite within the first five days of employment, otherwise their access will be disabled immediately.

When an employee leaves the Council, their user account and access to computer systems and data will be disabled automatically after the employee's last working day. This is initiated by the Council's Human Resourses (HR) team. After 1 week, their account and data will be deleted by the DDaT Service Desk. It is the responsibility of the personnel section within each Directorate to request this deletion using the Starter and Leavers form via the Self-Service portal and to also contact HR.

Similarly, personnel sections within each Directorate must inform the DDaT Service Desk when any staff changes job title/building location within the Council and/or moves to another Department/Team.

11.5 Administrator Access

The IT privilege levels assigned to staff must be commensurate with the tasks they are expected to perform. Local Workstation Admin, Domain Admin, Enterprise Admin and Microsoft 365 Admin Roles will be assigned to key staff and must be restricted to fully trained essential staff only.

11.6 External Connections to the Network

Every staff member has remote access to our network via official Council provided laptops using a secure VPN connection. Access to user accounts is by two factor authentication consisting firstly of a username and password and secondly a passcode generated using an authentication app. Only when both are satisfied is access granted.

11.7 Suppliers' and External agencies' access to the Council Network

Partner agencies and/or third-party suppliers that support IT systems must initially contact the DDaT Service Desk to be setup for remote access to the Bury Council network.

IT access is setup for each external supplier once they have provided the necessary company information and system access requirements.

Once setup and enabled, two factor authentication is required to access the account. When the account is not in use, for security reasons, the account is disabled.

Any changes to, or request for a supplier connection or disconnection must be sent to the DDaT Service Desk so that access can be applied or ceased. All permissions and access methods must be controlled by the DDaT Service Desk. No partner agency or third-party supplier should be given details of how to access the Council's network without the formal approval of the DDaT Service Desk manager.

The disclosure of connectivity details without the formal approval of the DDaT Service Desk manager will be considered a breach of the Council's Security Policy and must also be reported to the Council's Data Protection Officer.

11.8 Fault Logging

You must report all apparent faults with that use computer services to the DDaT Service Desk, who will issue you with a unique call reference number. This call number should then be quoted in any subsequent communication regarding the incident.

11.9 Change Control

When implementing any change to IT equipment or software used in the provision of any agreed service, the DDaT unit will maintain and follow change control procedures to ensure minimal disruption to service.

The DDaT unit will ensure that:

- changes are evaluated within a test environment, when possible, and implemented using change control procedures.
- compatibility is maintained between the changed item and all related hardware and software (whether operating system or application software).
- changes are scheduled to minimise risk to the operation of services.

Where a major system change is required on a customer's system, the DDaT unit will agree an implementation date with the customer in advance, after first assessing any impact on other related services.

The DDaT unit must ensure that advice is provided to departments to ensure that no requested change compromises security, IT standards, IT Strategies, other relevant codes, policies or standards, or conflicts with other user demands.

Where the DDaT unit wishes to implement a change that requires a period of downtime for any service, or alters the usage of the service, the DDaT Service Desk will notify all users for that system or the system's key users in advance. These key users must then notify all other users of that system within their department/team.

12 Physical Security

12.1 Central Computer Suite

Environmental Control

- The Central Computer suite **must** have environmental controls to detect fire, flooding and fluctuation in humidity and temperature.
- Emergency 'power off' facilities **must** be available in the Central Computer Suite.
- UPS (Uninterrupted Power Supply) **must** be in place to avoid failure following power surges or outages.

Physical Access control

- The Central Computer suite doors **must** be always secured and access restricted to authorised personnel only.
- A log **must** be kept of all visitors, maintenance and engineering staff given access to the Central Computer suite.
- All visitors to the Central Computer Suite **must** have specific Council visitor badges and be always accompanied.
- Employees **must** bring to the attention of their line manager any unauthorised access to the Central Computer Suite.
- Employees **must** not transfer identity cards or access fobs to unauthorised personnel.

- All known breaches of security in the Central Computer suite **must** be reported to the DDaT Service Desk, who will inform the relevant officers. Such incidents include:
    - Emergencies and disasters such as flood, fire, power failure and theft.
    - Any suspected security violations
    - Any suspected sabotage attempts
    - Computer virus contamination

12.2 IT Equipment located in Departments

- The Council's departments **must** ensure that doors and windows are properly secured.
- The Council's departments **must** not allow such equipment to be moved, modified, maintained, or repaired by any person other than those authorised or approved by the DDaT unit.
- All servers and IT communications equipment **must** remain switched on. Such equipment should be properly identified and marked.
- Access codes to the Council's buildings **must** not be disclosed to unauthorised personnel.

12.3 IT Equipment in Public Access Areas

Where equipment is located within areas open and freely used by members of the public, or in insecure offices and left unattended for periods of time; then particular measures must be taken to make the equipment as secure as possible e.g. secure it to the work surface.

13 Equipment Security

Equipment should be sited:

- To avoid unauthorised access or theft; workstations managing sensitive data **should** be positioned to eliminate the risk of overlooking.
- To reduce risks from environmental hazards: heat, fire, smoke, water, dust, vibration, chemical effects, electrical supply interference and electromagnetic radiation.
- Key safes **need** to be in staff offices.

Equipment should not be located near windows, where possible.

Appropriate safety equipment should be installed, such as smoke and heat detectors, fire alarms, fire extinguishing equipment and escape routes. Safety equipment should be checked regularly, in accordance with manufacturers' instructions and Health & Safety procedures.

Floor inspections of offices scheduled to take place on regular basis.

13.1 Personal use of the Council's IT equipment

IT equipment is provided primarily for business-related tasks only, but with the prior agreement of your line manager, you may be permitted to use the equipment in your own time for personal use. You may be required to contribute to the cost of computer consumables in respect of personal use.

However, you **must not** use Council-owned equipment to store personal files e.g. photographs, music and movie files etc. Storing these files takes up valuable Council resources and can seriously hamper the recovery of Council data in a disaster recovery situation.

13.2 Using Council's Equipment Remotely

When allowing IT equipment to be taken off-site, you must ensure it is insured under the Council's All Risks policy.

The provisions of this Policy apply to the use of IT equipment used offsite from Council premises and users must be made aware of their responsibilities when taking IT equipment off-site.

If any inappropriate material is found on computers or work smartphones, the line manager must be informed immediately. The Council reserves the right to inspect and recall IT equipment at any time.

If, by the misfortune of Council laptops being lost or stolen, they will be built from new with the recommended encryption solution and have their hard drives fully encrypted to safeguard the data stored on them.

13.3 Users' Responsibilities

Adequate steps must be taken to ensure the physical safety of IT equipment and the safety of any data stored on it. This applies to computers, smartphones and any removable media, including pen drives, CDs, DVDs, digital camera memory cards and digital pens etc.

Council computers must not be taken outside of the UK and connected to the Council's network via VPN without authorisation. This also applies to signing in to your Council Userid from outside the UK. Performing either without authorisation will be detected which then creates an IT security incident and investigation. Anyone needing to work outside the UK for a specific purpose, please contact the DDaT Service Desk.

13.4 Advice on the use of pen drives, CDs, DVDs and other portable devices

External storage devices such as pen drives should not be used. There is no case, given the introduction of Microsoft Teams, OneDrive and SharePoint, for computer files to be held on removable media such as pen drives, data storage media and other portable devices.

Do not store confidential/sensitive information on these devices. If information is being stored on such devices, then delete the confidential/sensitive information from devices as soon as possible.

You are personally responsible for the safety of any Council information/data you store on such devices.

14 Glossary of Terms

App or Application - The name given to a software programme or set of programmes to do a specific task.

Back-up - A copy of data/information which can be retrieved in the event of the original data becoming deleted, accidentally overwritten or corrupted.

Data - Information held in computer readable format that is processed by computer programs.

Data encryption - Data is held in a scrambled (ciphertext) format, which cannot be made readable (plaintext) unless the correct access is used. Encryption is used to maintain the confidentiality of data during storage or transfer between IT systems.

Development Application - The programmes and data files used to run a specific application in a "test" environment.

DPO - Data Protection Officer.

Downloads (Internet) - The acquirement of software and or other data onto the computer directly from the Internet.

Email - The sending and receiving of messages and files over computer networks between individual mailboxes. Any user with appropriate software and equipment can send and receive.

Executable Code - An instruction or set of instructions in a format which the computer operating system can interpret and execute.

File Server - A powerful computer, which is used to electronically store and retrieve documents across the network.

Firewall - A security system that controls information and traffic across the internal network and to external networks.

FOI - Freedom of Information.

Hardware - A piece of computer equipment.

IAO - Information Asset Owner.

IAM - Information Asset Manager.

IT Change - The procedures followed by the DDaT section whenever a Control Change is made to an IT system.

Line Monitor - A piece of equipment used for fault investigation to monitor data across the network.

Live Application - An application which uses live data as opposed to test data.

Media - Items used for storing data, for example tapes, CD-ROMs, DVD optical discs. Back-up media is used to retain extra copies of data, for use if the original data is lost or corrupted.

Network - The collective name for items of computer equipment linked together, including file servers, workstations and other devices, enabling communication between them.

Password - During sign on to a computer system, a user must provide a Userid, and known alphanumerical text associated only with that username before access to the system is granted.

Programme - A set of instructions that can be understood by a computer.

Public Domain Software - Software not subject to copyright. The author has placed the software in the "public domain" for free use.

SAR – Subject Access Request.

Secure Area - An office or area with restricted access. Only people with keys or "access fobs/codes" are allowed into the area.

Shareware Software - Software, subject to copyright and/or restricted features, for use on a "try before you buy" basis. After a specified period and/or to unlock full access, the software should be registered with the distributor and a licence fee paid.

Sign on - The initial entry point to a computer system. The user must enter a valid Userid and password to gain access.

SIRO – Senior Information Risk Officer.

Software - Programmes which run on a piece of computer equipment.

Standalone computer - A computer that is not physically connected to the network.

System Owner - The officer responsible for a specific system.

Userid - Each user of an application or computer is identified by a username. To gain access at sign on, the operator must provide a valid username and password.

Viruses – so called because they behave like biological viruses and can replicate or evolve without the user's knowledge. They can be relatively harmless or very destructive, for example, deleting contents of a hard drive.

Workstation – A computer and computer monitor for example, through which users can input or access information.

Appendix A – Personal Commitment Statement

I, _____ confirm that I have read and understand the attached policy and confirm that I will adhere to all its requirements.

Print Name:	
Signed:	
Date:	

Personal Commitment Statement

Introduction

The Authority's comprehensive IT Security Policy covering all aspects of IT Security is published on the intranet. This Personal Commitment Statement provides a summary of the key points as they apply to individual staff.

All staff who use the Council's DDaT facilities must agree specifically that they have read and understood what is expected of them, as detailed in this summary document.

All the points included in this document are covered in greater detail in the IT Security Policy – the Policy is regularly updated with information on significant changes sent out to all staff. **It is your responsibility to familiarise yourself with this Policy. New employees should ask their line manager to make the policy available to them within the first week of employment**.

Each employee is personally responsible for the confidentiality, security and accuracy of information and information systems they use as part of their job, whether working at a Council location or at another site, or at home. You must not attempt to access any IT system that you have not been given explicit permission to access.

All Council representatives should bear in mind that information they share through social networking applications, even if they are on private space, is still subject to Copyright, Data Protection, Freedom of Information, the Safeguarding Vulnerable Groups Act and other legislation. They must also operate in line with the Council's Code of Conduct and Equality and Diversity Policy. Failure to comply with the guidelines detailed here may lead to disciplinary action and/or legal proceedings.

We all have a responsibility for keeping Council data secure and using facilities sensibly; this document gives brief guidance on basic information security, covering the points below:

- Passwords.
- Desk Security.
- Security classification: Protective Marking.
- Third party requests for sensitive or personal information.
- Sending sensitive or personal information by email.
- Sharing Personal Data.
- Sending confidential information on CD/DVD, memory stick or other portable media.
- Advice on use of USB pen drives, CD/DVD, and other portable devices.
- Email use and Internet access.
- Remote working/home working.
- Secure Disposal.
- Other security issues.

If you need more detailed guidance, read the IT Security Policy or contact the DDaT Service Desk for advice.

Passwords

- Passwords **must** be a minimum of fourteen (14) characters and be based on 3 Words or a phrase. This creates a more memorable, longer and stronger password. The password needs to consist of a mixture of upper- and lower-case letters and/or numbers/symbols. You **must** avoid the use of passwords based on names of family members and pets, car registration numbers and simple patterns of letters from a computer keyboard. Please note, that you should **never use any derivation of the word 'password' as your password**.
- Passwords **must never** be disclosed to anyone. Keep your password secure and private.
- The use of another person's Userid and Password is not allowed.
- Temporary passwords **must** be changed at the first sign on.
- Passwords **must not** be written down.
- Passwords **must** be changed immediately if it is suspected or known that it has been compromised, and the matter reported to the DDaT Service desk. The compromised password **must** never be used partly or in full for any future password.
- Passwords **must not** be included in any automated sign on procedures, macros or function keys.
- **Do not** use the same or similar password for your Council work password that you use for personal accounts. Keep personal and Council work passwords totally separate.

Desk Security

- **Do not** leave confidential files or papers unattended on your desk – always store these securely.
- **Do** use the screen saver lock (press the Windows key and L) or sign out of your session if you are working away from your computer.
- **Do** make sure that confidential information displayed on your screen is not seen by others.
- **Do not** remove equipment or information without the appropriate approval.

Security Classification: Protective Marking

All routine public sector business, operations and services should be treated as **OFFICIAL**. There is no requirement to explicitly mark routine **OFFICIAL** information. Baseline security measures should be enforced through the Council's business processes.

Official-Sensitive – Is a limited subset of **OFFICIAL** information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the '**OFFICIAL**' classification tier but may attract additional measures (procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know' assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**.

Third Party Requests for Sensitive or Personal Information

Be incredibly careful if you receive an unexpected request from a third party (an organisation or individual outside the Council) for personal data we hold. Some individuals make a business out of, and are very skilled at, obtaining personal data under false pretences. Consult with your line manager when dealing with any unusual requests.

- If there is a business rule to deal with such situations (e.g. requests for Council Tax data), follow it! If there is not one in place, check with your Head of Service.
- Satisfy yourself that the person is who they say they are.
- Ask for the request in writing.
- Take a phone number (preferably a switchboard number, not a direct line).
- Keep a record of such requests.

Sending Sensitive or Personal Information by email

This type of information should only be sent by email where there is no reasonable alternative and where not sending the information would cause a significant problem for a service user/customer.

When sending an email under these circumstances, the guidelines below **must** be followed:

- **Do not** send emails and attachments containing sensitive information to a generic email address e.g. info@bury.gov.uk; the email address should be a named individual.
- Make sure that you have sent data to the right person and check that they have received it.

- To increase the security of information sent, encrypt the email in Outlook using 365 Encryption. If including a file attachment, add them to a 'zip' file and password-protect the zip file. The password can then be passed to the recipient by phone, or an alternative is to share the file from OneDrive or SharePoint with the recipient and add the file link to the email. Contact the DDaT Service Desk if you need advice on this.

Sharing Personal Data

There are many situations in which we share personal data within the Council and with external organisations including central government. These range from 'one off' requests to formal arrangements. We only do this where we have a legal power or duty to do so, and the sharing must meet the conditions of the Data Protection Act. Sharing data may itself create an information security risk which needs to be addressed. If you are not sure whether you should be sharing information, consult your line manager for guidance or our DDaT Service Desk for further advice.

Sending confidential information on CD/DVD, USB pen drive or other portable media

You **must not** send confidential information via portable media, even if the data is encrypted. Instead follow the guidelines above for sending via email.

Advice on the use of CDs/DVDs, USB pen drives and other portable devices

External storage media and devices **must not** be used. There is no case, given the introduction of Microsoft Teams, OneDrive and SharePoint, for computer files to be held on removable media such as pen drives, data storage media and other portable devices.

- **Do not** store confidential/sensitive information on these media and devices.
- **Do** delete confidential/sensitive information from these devices.
- **You are personally responsible for the safety of any Council information/data you store on such media and devices.** If you remove it from Council premises, then you are responsible for ensuring its safe transport.
- If you lose the media or device, report the loss to your line manager and/or the owner of the data immediately.

Email and Internet Use

- You may make limited private use of the Council email system for personal needs – but this should be limited and in your own time, in accordance with the ICT Security Policy. However, any personal mail may be subject to recording and monitoring, as with business mail, so **you should have no expectation of privacy**.
- You may access the Internet for personal use in your own time via the Council's network. Normal internet filtering rules are relaxed between 12 and 2 pm to facilitate this. You should again bear in mind that **this personal use is subject to recording and monitoring**, as with business use.
- You **must not** register on any non-work-related websites or distribution lists using your Bury Council work email address.
- Council data **must not** be sent to and from an employee's personal non-work email account.

- Personal non-work email accounts **must not** be used to conduct or support official Council business. All emails that are used to conduct or support official Bury Council business **must** be sent from a Council email address. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Remote Working and Home Working

- **Do not** keep any sensitive or confidential information or anything that you do not want to see in the public domain on a CD/DVD, USB pen drive, computer or any other mobile device.
- **You are personally responsible** for any Council information you take out of the office.
- The only place where confidential or sensitive electronic information should be held is on the Council network.
- **Do not** leave the information unattended.
- **Do not** leave information in a car where it can be easily seen.
- If you need to work from home or out of the office on a regular basis, you must get authorisation from your line manager. Contact the DDaT Service Desk for more information about remote working.
- If you are working from home, you **must** comply with the policies on Individual Home working (ad-hoc home working) and the Remote Working Policy (permanent home-working). In particular, the policies state:
  "Employees working from home have the same responsibilities under the Data Protection Act to ensure all data is kept secure. Employees should ensure that no members of their family use Council equipment. They should also ensure that any documents are stored securely, particularly those containing personal data, which should be stored in a locked cabinet. Managers should ensure that employees are aware of their responsibilities and that any breach of security would result in disciplinary action being taken against them."

Secure Disposal

- **Do not** put papers which are **OFFICIAL-SENSITIVE** into the recycling bins. **Do** put them into a confidential waste bag for secure disposal.
- If you are disposing of pen drives, CDs, DVDs and any other electronic devices, **do so securely**, so that the information previously stored on them cannot be recovered. This can be done by arranging delivery of said items to the ICT Service Desk. **Do not** place any of these portable devices in the rubbish bin.
- If you are disposing of a computer, please arrange delivery of the item to the ICT Service Desk so that the device`s hard drive can be wiped in accordance with the Council`s policy regarding the disposal of IT equipment (see the ICT Security Policy for details).

Other Security Issues

- **Do not** disable anti-virus/malware protection installed on equipment.
- **Do not** do anything which could introduce a virus or spyware onto Council provided computers, devices and emails which could then propagate to the network.
- If at any time you suspect that your computer is behaving oddly and may have been infected with a computer virus or other malicious software, **you must immediately contact the DDaT Service Desk to report a potential security incident.** The DDaT Service Desk will provide immediate advice on any action needed to prevent the spreading of virus infection and will arrange an urgent visit from support staff if appropriate.
- If you become aware of any significant breach of the Council`s IT Security Policy (e.g. sharing/disclosing personal passwords or abusing personal information) **you should immediately inform your line manager and Internal Audit and/or the DDaT Service Desk, as appropriate.**
- When leaving the Council's employment, you **must** return all council property to your line manager (laptop, mobile phone, home IT equipment, USB pen drives, keys, photo ID badge and security fobs/access tokens etc.). You **must** also remove your Council work email profile and any other related accounts from any personal computers and mobile devices that you have installed it on.