ICT Use and Security Policy

A group of people in a circle

Description automatically generated A hand and heart in a circle

Description automatically generated A purple circle with a white outline of a thumb up

Description automatically generated A white outline of handshake in a pink circle

Description automatically generated A green circle with a white outline of a person and a check mark

Description automatically generated

|  |  |
| --- | --- |
| **Date created** | *October 2018* |
| **Version** | *14* |
| **Author** | *Leon Thomas Technical & Infrastructure manager* |
| **Department - Section** | Strategy Policy and Transformation |
| **Date last reviewed** | *October 2023* |
| **Policy review next due** | *January 2024* |

Document History

Version Control

|  |  |
| --- | --- |
| **Organization** | Description |
| Title | Corporate Information Security Policy |
| Filename | ICT Use and Security Policy Version 14 |
| Owner | Suzanne Jones - Strategic director Customer, Business and Corporate support – SIRO |
| Subject | ICT Use and Security Policy |
| Protective Marking | Protect departmental |
| Review date | August 2023 |
| Next Review Date | January 2024 |

Document Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Date** | **Revisor** | **Previous Version** | **Description** |
| 22/10/2018 | Simonne deVall | V9 | HOS full review |
| 30/11/2018 | Caroline Croft | V10 | Feedback from CEXB |
| 01/04/2019 | Simonne deVall | V11 | Final review |
| 01/01/2021 | Simonne DeVall | V12 | Final review |
| 18/02/2021 | Caroline Croft | V12.1 | Amended for links for loading into SharePoint. |
| 17/11/2022 | Leon Thomas | V13 | Full review |
| 12/05/23 | Leon Thomas | V13.1 | Updated section 13.1 |
| 20/07/23 | Leon Thomas | V14 | Updated |
| 18/07/23 | Leon Thomas | V14.1 | Updated section 7.7, 13.1 and Section 28 |

Table of Contents

[1 Definitions 3](#_Toc62483966)

[2 Introduction 5](#_Toc62483967)

[3 Scope 5](#_Toc62483968)

[4 Information Security Roles and Responsibilities 6](#_Toc62483969)

[5 Monitoring 10](#_Toc62483970)

[6 Access to ICT services 11](#_Toc62483971)

[7 Acceptable Use of ICT Services 12](#_Toc62483972)

[8 Breaches of Policy/Reporting incidents 21](#_Toc62483987)

[9 Privacy Regulations 22](#_Toc62483988)

[10 Safety when using ICT equipment 23](#_Toc62483989)

[11 Physical Security 23](#_Toc62483990)

[12 Network Security 26](#_Toc62483991)

[13 ICT Asset Management 27](#_Toc62483992)

[14 3rd Party Supplier Management 28](#_Toc62483993)

[15 Change Control 29](#_Toc62483994)

[16 PCI DSS 29](#_Toc62483995)

[17 Human Resources Information Security Standards 30](#_Toc62483996)

[18 Legal Responsibilities 30](#_Toc62483997)

[19 Legislation 31](#_Toc62483998)

[20 Communications and Operation Management 32](#_Toc62483999)

[21 Policy Compliance 32](#_Toc62484000)

[22 Policy Governance 33](#_Toc62484001)

[23 Business Continuity Planning 33](#_Toc62484002)

[24 Review and Revision 34](#_Toc62484003)

[25 Appendix A - Constraints on using GSCX mail and Personal Commitment Statement 35](#_Toc62484004)

[26 Appendix B – Password Policy 38](#_Toc62484005)

[27 Appendix D - E-Mail Out of Office Template 40](#_Toc62484006)

[28 Appendix E – How to send encrypted mail 41](#_Toc62484007)

[29 Appendix F: Last Person Out routine 41](#_Toc62484008)

[30 Appendix G: Reporting a lost phone 41](#_Toc62484009)

[31 Appendix H: Data categorisation 41](#_Toc62484010)

Definitions

|  |  |
| --- | --- |
| Term | Definition |
| Data | Data is raw, unorganised facts that need to be processed. Data can be something simple and seemingly random and useless until it is organised. |
| Information | When data is processed, organised, structured or presented in a given context so as to make it useful, it is called information. |
| Information & Data Assets | All information must be considered an asset which includes printed and written documents, reports and letters.  All the data assets we hold have been identified and classified under the new GDPR regulations and stored in the following location  G:\GDPR\Revised Information Record & Disposal Schedules\Information Logs 2022 |
| IT Security/Cyber Security | IT security and cyber security is the body of technologies and practise design to protect networks, programs and data from attack, damage or unauthorised access. The overarching aim is to ensure confidentiality, integrity and availability of data and ICT systems. |
| Information Security Management System (ISMS) | A systematic approach to managing sensitive council information so that it remains secure. It includes people, process and ICT systems by applying a risk management approach. |
| Anti-Virus/Malware protection | Software that provides an electronic defence mechanism mitigating the risk of a computing device being infected with or affected by malicious intent/content. |
| PSN | Public Secure Network. A secure data network provided by the government and use by government organisations to communicate over, and exchange data securely. |
| Data Transfer Mechanism | Mechanisms by which data can be securely transferred between bodies. |
| Personal Data | Please see Appendix H |
| Sensitive Personal Data | Please see Appendix H |
|  |  |
| Media | Media is considered to consist of the following items removable media, such as CD-ROM/CD-RW discs, USB. |
| ICT equipment and Services | These include but are not limited to   * Personal Computers * Laptops * Tablets * Phones and smartphones/Samsungs * Corporately provided network and network equipment * Printers * Scanners * Cameras |
| ICO | Information Commission’s Office  Government body responsible for ensuring that organisations in the UK adhere to the standards required when handling customer data. |
| CMDB | Configuration Management Data Base (Held on Salesforce)  (Asset register for all ICT assets) |

Introduction

The purpose of this policy 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 confidentiality, integrity and availability of the information used and produced.
* Business damage and interruption caused by security incidents is minimised.
* All legislative and regulatory requirements for handling data & information are met.
* The Council's ICT equipment and facilities are used responsibly, securely and with integrity at all times.
* The Council protects against all threats both internal and external to the data we hold across all the applications we use.
* Staff are aware of their responsibilities under this policy and have the necessary information to allow them to use the ICT services safely and securely, protecting them from risk of personal liability for accidental misuse or loss of data & or information

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned by and held by the Council:

* Ensuring all staff are aware of and understand their responsibilities under this policy
* Describing the principles of security and explain how they apply
* Introducing a consistent approach to security across the organisation
* Creating and maintain a level of awareness of the need for Information Security vigilance as an integral part of day to day business
* Protecting information assets by establishing proportionate controls over its use and distribution

Scope

Information stored in the computer systems owned or used by St Albans City and District Council (the Council) is a valuable corporate asset. Having this information comes with a growing risk of it being misused, lost or damaged through accidental or malicious intent.

This policy applies to all persons authorised to use the Council’s computer systems and communications network, including but not limited to employees, casual staff, councillors, contractors, consultants, voluntary organisations and suppliers granted access for support or information sharing purposes.

Non-compliance with the policy is regarded as a serious matter and may result in disciplinary or legal action being taken.

Information Security Roles and Responsibilities

The table below sets out the responsibilities of the user groups in the organisation in relation to the production and implementation of the guidelines in this document.

Specific Roles

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Holder** |
| Chief Executive | * Ultimate responsibility for information security covering all areas of the council. | Amanda Foley |
| Senior Information Risk Owner | * Responsible for the review of this policy and ensuring that it underpins our approach to managing the ICT environment. | Suzanne Jones |
| IT Manager | * Responsible for the creation (and regular review) of this policy and ensuring that it underpins the Information Security Management System approach. | Leon Thomas |
| OD Manager | * Ensuring all managers are aware of their specific responsibilities under this policy. * Ensuring that the corporate training covers the key security messages. * Ensuring that the policy is sent to all persons joining the company ahead of their start date. * Reporting and acting on non-attendance of mandatory training. | Jane Pearce |
| System Owners | * Responsible for ensuring that the operational guidelines as set out in Section 7 apply to the management and operational processes of systems they are responsible for. * Ensuring that the applications they manage are kept up to date, are on the latest versions at all time, ensure adequate budget provisions is availed to maintain the application. * Work with the ICT to address any failures of the applications identified from audits, external security testing for example annual penetration tests. * Ensuring that the necessary application operating processes are in place to maintain the integrity, availably and accuracy of data held in their applications. * Ensuring that access to the data held in the systems they own, is limited to “needs only”. * Manage 3rd party access to the guidelines as set out in Section 13. | All System Owners |
| System admins | * Ensuring compliance with Section 7 when performing the administration for their system(s). | All system admins |

General Roles

|  |  |  |
| --- | --- | --- |
| Role | Responsibilities | Holder |
| Strategic Director/Principal Officers | * Ensure there is a culture of adherence to this policy by incorporating key messages into service and processes design and implementation. * Ensuring that the GDPR information asset register, and disposal schedules are kept up to date, accurate and acted-on. * Ensuring that adequate budget provision is made each year to support necessary application/environmental upgrades. | Officers grade PO1 and above |
| Managers Responsibilities | * Ensuring all new starters have signed the ICT Security Policy, should not be provided access to the network until the policy has been signed and returned. *Note: Managers who request user access before the ICT policy has been signed, do so at their own risk and are responsible for the actions of their staff until the policy has been signed.* * Ensuring the staff are aware of how to report security incidents or data loss/ data breaches / loss of equipment * Ensuring staff understand the principles of data asset management. * Ensure that access to customer data and information is appropriate to the role being held by each member of staff. * Supporting System Owners, Administrators and ICT teams in the enforcement of the ICT Security Policy. * Ensure staff complete all mandatory security training. * Requesting that the ICT creates computer accounts for new staff before they take up their employment with the Council. * Informing the ICT services desk of people leaving their employment and providing adequate notice * Arranging for the return of all ICT equipment peripherals, and removable media from leaving staff. * Notifying ICT of long-term absences (28 days or longer) so that accounts can be disabled appropriately. | Officers with staff management responsibilities |
| All Staff Responsibilities | * Reading and signing the ICT Security Policy. * Considering the sensitivity of the information they handle (with personal and sensitive information. about vulnerable people being the most important). * Protecting information in proportion to its sensitivity by complying with the Data Protection Act and the General Data Protection Regulations (GDPR). * Reporting security incidents or data loss/ breaches in accordance with the ICT Security Policy. * Reporting loss of equipment. * Complying with the departments data handling and retention schedules. * Comply with the Council’s protective marking policy. * Ensuring that information, whatever it’s format, is secured by physical means (e.g. locking paperwork away) or by using approved electronic means (e.g. only using Council IT equipment). * Ensuring changes to shared information are updated as soon as possible on the primary record location or system (not kept at home or personal storage not accessible to others). * Ensuring that all equipment, peripherals and removable media supplied by the council are returned to the IT department before/on the last working day of your employment. * If planning to work outside of England or Wales, checking with, and obtaining written approval from your manager and ICT manager prior to re-locating your work space. | All Staff |

Monitoring

The Council provides ICT systems for council business use. There are no automatic rights of personal use, or individual privacy.

Use of the Council’s business network and services is monitored at all times.

The Council reserves the right to use the information in the system logs for the below purposes:

* Ensuring compliance with the council’s operating standards, business process, procedures, and policies
* Investigation of cyber, criminal and data breach or data loss incidents
* Performance management
* Provision of usage data to support staff training needsm
* Adherence to the council’s legal obligations
* Preventing or detecting inappropriate unauthorised use of the Council’s ICT infrastructure and systems.

In the event of suspicion of misuse of the Council’s network and services, information held in the Council’s systems and logs may be shared with HR, Audit, Senior Managers and other investigative bodies for example the police as required to support any investigation.

Guest internet access is available for personal email and other social media use with the expectation that staff use their own devices for this purpose.

Note: Internet access on the guest network is not monitored however please be aware that the guest network is limited in terms of access to pornographic, drugs, racist, hatred and terrorism sites being barred.

Access to ICT services

Cybercrime is undertaken (generally) by 5 bodies

* Nation States
* Organised Crime
* Cyber Criminals
* Scammers & Phishers
* Disruptive individuals

We have various technical resources to help protect against most threats. However, the Council is connected to central government and therefore it might be possible to breach our security and gain access central government where the gains of disruptive cyber activity may be lucrative.

As there is uncertainty about technology outside of the EU, remote access to the Council’s network is granted from within the UK and EU region only and technical controls are in place to limit network access from outside this region.

Under no circumstances staff must not:

* Take equipment (including phones) to high-risk countries such as China or Russia (it may be inspected and infected on entry to the country)
* Allow data access from any source or equipment (including works supplied phones) to be attempted from level 1 countries such as Russia, China, Syria, Vietnam, Ukraine, Belarus, North Korea, and Iran. (Voice services may be permitted but only on request)
* Work from any country outside of England and Wales

If there is a need to be contactable whilst travelling into countries outside of the EU, please contact ICT for advice and guidance.

Please note:

* You will have to have HR and HOS approval to work outside of England/Wales.
* Access from outside of England & Wales is disabled by default and only enabled on receipt of the proper approval

Acceptable Use of ICT Services

This section sets out the standards of ICT usage that all staff are expected to adhere to when using the ICT network and environment.

Account Management

Passwords that only use dictionary words such as “CoffeeMorning” can be cracked in minutes.

All staff must use complex password which are non-related words, combined with numbers and symbols.

The best kind of password would be XKJ@12fjpo!9

You are responsible for the strength and security of your password by:

* + 1. Changing your password(s) after first successful log to be complex, and to maintain the complexity throughout your employment. See Appendix B for details
    2. Not using your name, day of the week, month, year, the word “Password”, your children’s name, your pets name, or anything that is easily identifiable to you, such as your car registration, make colour etc.
    3. Ensuring that “Clearview” password functionality is turned off so that passwords not displayed when typed into any password dialogue box;
    4. Not using passwords that you use for your personal accounts, at work to avoid a cross-organisation attack. (See Definition)
    5. It is a user’s responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems. Do not write down, mutter your password when entering it or share it with another user (outside of the ICT team)

What to do in the event of a security issue

If you suspect, you may have been subject to a malware or virus attack you must do the following actions with immediate effect:

* + 1. Shut your device down by holding down the Power off button. Speed is of the essence when dealing with a virus/malware issue – do not save your work first, shut the device down first.
    2. Immediately inform ICT who will take the appropriate action.
    3. If you suspect your password may have been compromised, then please change your password immediately and advise ICT who will check to see your account is being used from elsewhere.

Use of Equipment

* + 1. When using equipment supplied by the Council the following guidelines must be adhered to:
    2. Equipment left unattended by the user must always have the windows software lock applied (CTRL+ALT+DEL and LOCK) as a minimum, and ideally shutdown completely.
    3. Equipment used to store or transmit Council data must always be encrypted – this includes mobile phones and tablets and protected by the Council’s Mobile Device Management solution (Either SCCM or Intune) and be appropriately secured through password strength enforcement.
    4. The Council does not operate a ‘Bring Your Own’ Device (BOYD) scheme – only equipment supplied by your ICT department must be used for works purposes.
    5. Do not leave equipment completely unattended. If no other member of your team is in the vicinity please take the device with you, or, lock away in a cupboard or locker.
    6. Any loss of equipment must be reported immediately to the ICT service desk (Extension 6999), line manager and departmental administrator.
    7. Any loss of phone equipment must be reported immediately to Vodafone, so that the SIM can be disabled to prevent usage as well as line manager and departmental administrator. Please see Appendix G for Details.
    8. When working outside of the office, be aware of your surroundings. If you are working in a public place, ensure that your screen cannot be overlooked, or your phone calls overheard. If it is not possible to work without being overlooked or overheard, then it is not considered safe to continue working.
    9. When working in the office be aware of visitors working in your area. Ensure that your screen cannot be overlooked, or your phone calls overheard by the visitor. If this is not possible consider moving to an alternative area in the office.

Remember: You are responsible for equipment issued to you. If you lose your device report it immediately to minimise the risk of someone using the device maliciously.

Data Handling Policy (Do’s and Don’ts)

Do’s - When handling St Albans data, or using the ICT services you must:

* + 1. Only access the Council’s systems for legitimate business purposes.
    2. Only handle customer information appropriate to the role being performed. Note: If you realise that you have access to data inappropriately you must notify your manager immediately.
    3. Never permit others to access or use your individual computer account without supervision by yourself.
    4. If you share your desktop with another party (Teams, Zoom, GoToMeeting etc) never leave the session unattended and monitor the activity of the person accessing your device.
    5. Never disclose your individual computer account password in any form (Written or verbally – other than to the St Albans ICT team).
    6. Always ensure that any temporary data used for reporting and/or other purposes is deleted within an appropriate timescale for the task being performed (please refer to GDPR data sheet).
    7. Ensure that when sharing data either internally or externally via any channel that the recipient is :-
    8. Valid – data breaches commonly happen due to staff accidently sending information to the “wrong” David for example.
    9. Has the correct level of authorisation to view the information being shared?
    10. The data in its entirely, is appropriate to be shared with the recipient.

Don’ts - When handling St Albans data, or using the ICT services you must not:

* + 1. Never leave your device unattended, without locking your workstation (CTRL+ALT+DEL and LOCK) unlocked and unattended.
    2. Use any Council services to access, convey, share or store profane, libellous, illegal, pornographic, racist or hatred material on any machine, storage device or service owned by or used by the Council.
    3. Access profane, libellous, illegal, pornographic, racist or hatred material via the Internet, e-mail or handled via any other electronic device owned by the Council.
    4. Process any privately-owned information or store private information on Council owned equipment and/or storage services.
    5. Use the Council’s infrastructure to support private commercial activity of any kind.
    6. Use privately owned removable media without prior written permission from the ICT department and line manager
    7. Use equipment not procured by the Council on the Council’s network to access Council services and storage.
    8. Install or attempt to install any software onto Council supplied equipment.
    9. Attempt to access systems which you do not a legitimate right to access.
    10. Deliberately misrepresent yourself as another staff member from the Council.
    11. Use ICT services and equipment in such a way as to be seen to cause harassment of interference to either other employees or residents/customers of the Council.

Working Flexibly

Section 7.3 (Use of Equipment) sets out the controls staff need to follow when using Council supplied equipment. When working flexibly either from home or out of the office, the following additional guidelines must be followed:

* + 1. Do not leave your equipment in a vehicle wherever possible. If unavoidable – please ensure it is not in any way visible.

Ensure you are not overlooked or overheard. Never leave your device unattended without locking your workstation (CTRL+ALT+DEL and LOCK) unlocked and unattended.

* + 1. Do not leave your equipment near an open door or window, or where it could be easily taken.
    2. When not in use always power off your device.

Remember: Your device is ‘**your** **personal responsibility’**. Keep it Safe. Keep it Secure

Use of E-mail

Context: The use of e-mail is now prevalent in our everyday working life for most staff. The convenience and speed of e-mail can present a risk to the organisation; for example, by staff accidently sending data/information to the wrong recipient. It is very important that e-mail is used safely and securely by ensuring that:

* + 1. All e-mail is sent from an official Council e-mail.
    2. You use the corporate e-mail signatures (Full & Reply). See Appendix C for details.
    3. Under no circumstances you communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s Code of Conduct or Equal Opportunities policy.
    4. Where e-mail is available, this must be used for all external e-mail use and must be used for communicating documents that hold the OFFICIAL-SPECIAL CATEGORY PERSONAL DATA marking scheme.
    5. Automatic forwarding of email is considered carefully to prevent OFFICIAL-SPECIAL CATEGORY PERSONAL DATA material being forwarded inappropriately and must never be used to forward to an external recipient.
    6. Out of Office messages are in line with the Council’s template when not accessing emails for example when on leave. (Please see Appendix D for Out of Office Template).
    7. Use of personal E-mail (i.e. not @stalbans.gov.uk) to conduct council business is strictly prohibited.
    8. Use of Council’s e-mail address to conduct private / personal business is prohibited.
    9. All official external e-mail must carry the official Council disclaimer which for your convenience will be added automatically by the e-mail system.
    10. E-mails concerning Council business are official documents having the same legal status as a letter sent on letter headed paper. Care must be taken that the e-mail is aligned to Council standards for written documentation.
    11. E-mail is not a secure medium and encryption must be used when e-mailing SPECIAL CATEGORY PERSONAL data/information. (See Appendix E for details of how to send data securely).
    12. All e-mails that are used to conduct or support official St Albans District Council business must be sent using devices owned and deployed by the Council’s ICT team only devices.
    13. Gain written authorisation from the user’s line manager or Strategic director if a user needs to access a colleague’s e-mail, or other data not stored on the common drive. ICT will only allow limited and monitored access.

Care when using E-Mail

The receipt of SPAM, Junk e-mail and Phishing mails are a nuisance and, in some instances, a threat.

All users must be cautious about any potential unsolicited email and delete any at the earliest possible opportunity.

If you are suspicious of an e-mail, please report this immediately to the ICT Service Desk. Do not open any links in the document and press the phish alert report button in Outlook. Visit [here](https://stalbanscdc.sharepoint.com/sites/StaffNet/SitePages/Phish-Alert-Button-(PAB).aspx) for more guidance

Please refer to our online Cyber Security Training, which deals in detail with how to protect yourself from a Phishing attack.

Phishing tests are undertaken on a regular basis as part of our cyber security plan. Failing the test is a serious concern and you will need to complete mandatory online training. If you fail our simulated test twice your manager will be notified and will discuss it with you and informal action may be taken.  If you fail the test on a third occasion, your line manager will be notified once again and may consider further appropriate action.

Sending emails Securely

Take extra care when sending personal identifiable information externally by email and ensure you use the send secure option in [Zivver](https://stalbanscdc.sharepoint.com/sites/StaffNet/SitePages/Zivver(1).aspx). This will ensure the message is encrypted and you also have the option to recall the message if you accidently send it the wrong person.

Failing to send emails securely, which include personal identifiable information, which leads to a data breach could lead to action being taken by your line manager in line with the Council’s Disciplinary policy and procedures.

Use of the Internet

The Council is held responsible for actions taken by its staff whilst using the Internet. Staff have a personal responsibility for maintaining the reputation of the Council whilst using online services, especially when using social media and the internet in general.

Internet misuse may include, but is not limited to accessing, viewing, sharing, printing and downloading or similar actions.

When using the Internet staff must not:

* + 1. Create, download, upload, display or access knowingly, sites that contain pornography, terrorism, racist or other “unsuitable” material that might be deemed illegal, obscene, or offensive.
    2. Violate Copyright rules.
    3. Gain unauthorised access to other people/organisations networks.
    4. Engage in gaming, dating and/or gambling sites and software using the Councils equipment or services.
    5. Cause disruptions and/or harassment to others users work in any way either through distraction, offense, or via spread of malware/viruses.
    6. Express personal views that may be interpreted as being the official policy of the Council.
    7. Commit the Council to the purchase of goods and/or services without proper authorisation.

The above list is not exhaustive but is to provide guidance on acceptability standards.

In general, the test for acceptability is whether the staff member can reasonably justify their actions to a senior manager if requested.

* + 1. The Council reserves the right to deny access to websites that it feels violate the above principles or post cyber threat to the council (i.e. phishing sites)
    2. Managers are responsible for monitoring staff time spent in personal use of the internet and must raise issues with ICT / HR / line manager concerning excessive use, where there is reason for concern.
    3. Staff wishing to use the internet for study reasons must seek prior approval in writing from their manager.

Please be aware that access to the internet is always monitored.

Personal use of the internet must be

* + 1. Limited and outside of core hours.
    2. Not counted in flexitime/timesheet calculations.

Use of Software and Applications

There are very specific laws that apply to the licensing of software. These are regulated by FAST (Federation against Software Theft) but can also be audited by companies such as KPMG and Deloitte. Violation of licensing agreements can be very serious.

* + 1. They can be costly in terms of back dated licenses fees.
    2. Damaging in terms of the organisation’s reputation.
    3. Involve considerable amounts of officer time working with and responding to the demands of the auditing party.

To protect the organisation against violation of our software licensing agreements all staff must ensure that:

* + 1. All software procured by the Council is subject to licensing agreements that comply with the statutory legal requirements and software licensing laws.
    2. The ICT Team ONLY installs software onto corporately provided devices.
    3. Only software as a service product licensed by the Council is used.
    4. All software requests, or IT purchase requests are supported by an approved SERF [form](https://forms.office.com/r/WQz7GVmAtG) and the purchase and installation of software is undertaken by ICT. Any unapproved software requests must be approved by the approval manager and IT.
    5. Personal or unsolicited software is not loaded onto a Council equipment. This includes chargeable ringtones, wallpaper, or screen savers.
    6. No unauthorised changes are made to software.
    7. No attempt is made to disable or reconfigure the Personal Firewall software or anti-Virus software.
    8. Illegally reproduce software. Please note this can be subject to civil damages and criminal penalties and staff can be personally liable for violation of licensing and copy write agreements.

Use of Physical and Removable Media/Documentation

When handling printed or removable media the following controls must be followed:

* + 1. All 3rd party media must first be scanned and approved by St Albans ICT Team before being used.
    2. All data stored on removable media devices must be encrypted and stored on devices supplied by the St Albans ICT team.
    3. Damaged or faulty removable media devices must not be used.
    4. Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Service Desk so they can be securely disposed.
    5. Employees must return all removable media in their possession to their line manage when leaving the council, or transferring to a different role
    6. Any loss of removable media must be treated as a security incident and reported to the St Albans ICT team, line manager and departmental administrator straight away.
    7. The use of all non-Council issued removable media devices is forbidden. The use of removable media devices will only be approved if there is a valid approved business case. Note: Only media supplied by the ICT team can be used by staff and must be encrypted to FIPS140-2 standard and password protected.
    8. Passwords to media must be treated in accordance with our authentication password standards.
    9. Passwords for removable media must not be written down.
    10. Removable media must not be used to take information/data home, to then work on non-ICT supplied device (i.e., PC/Laptop). If you need to work from home, then the only acceptable form of home working is to be supplied with a laptop and VPN connection.

The following physical controls when creating or handling removable media and documentation must be applied:

* + 1. Ensure that personal information contained in documentation form, or on removable media is locked away when not in use.
    2. Media that holds personal information, or documentation considered commercially sensitive, or documentation relating to the political elements of the council must be disposed of appropriately and must not be placed in general waste.
    3. Paper copies must be placed in the confidential waste shredding bins situated throughout the building.
    4. All paper documents must be cleared away at the end of the day.
    5. Disks/USB keys must be returned to ICT for destruction/re-use.
    6. If you need to send media to another party special care must be taken. You must physically protect removable media devices and stored data from loss, theft, or damage e.g., consider sending media via recorded delivery.
    7. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device. You must be able to demonstrate that you have taken reasonable care to avoid damage or loss.
    8. Always ensure that the media and the encryption password are sent in different forms. For example – post the media, text the password to a mobile phone.
    9. Media holding and/or having stored PERSONAL SENSITIVE DATA information must be disposed of in accordance with the Councils Erasure and Disposal standards, using the following methods:
* Shredding - papers; extracted magnetic tapes, removable media.
* Incineration - paper, removable media (CD/DVD disks).
* Council approved agent - destruction and disposal of hardware equipment that complies with the Waste Electrical, Electronic Equipment Directive (WEEE Directive) regulations and disposal of removable media.

Use of Collaboration Tools

The Council’s Collaboration Tool is Microsoft Teams, OneDrive, and SharePoint. For the protection of the Council’s reputation and data security the following rules must be adhered to.

* + 1. All Council meetings scheduled by the Councillor must be conducted using Microsoft Teams, using the Council’s Office365 accounts.
    2. Meeting records must be made with consent from all parties in the meeting.
    3. Recording of meetings must not be shared (internally or externally) without permission from all parties.
    4. The use of other collaboration tools (such as Zoom) is permitted, but only to **attend** meetings scheduled by external organisations (For example Training). The use of collaboration tools other than Microsoft teams for scheduling council meetings/events is not permitted unless written permission is granted by the ICT manager, and department team lead.
    5. OneDrive is restricted to share files internally only
    6. SharePoint can be used for sharing files internally and externally.

Breaches of Policy/Reporting incidents

In the event of a breach in policy or detection of or suspicion of a security incident you must immediately contact:

* Your line manager and departmental administrator.
* IT manager, in accordance with the Council’s security Incident Management Policy (leon.thomas@stalbans.gov.uk).
* RING (do not e-mail) The ICT Service Desk immediately on Extension 6999 or 01727 819587
* The Council’s SIRO, via e-mail notification (gdpr@stalbans.gov.uk).

Report any incidents or suspected incidents immediately in line with the Responsible Reporting (Whistle Blowing) policy and Guidelines for Managers & Supervisors – IT Incident Reporting & Requesting Data about Email & Internet Usage.

Please note: Anonymity will be protected as outlined in the Council’s Whistle Blowing Policy.

Privacy Regulations

* Please be aware of people’s individual privacy when taking pictures and videos for Council use.
* Care must be taken to only include images of children where parental/guardian permission has been explicitly granted.
* In the case of ‘managed’ events, good practice is to announce at the start that pictures will be taken for promotional purposes, and to advise people at the event to please let the announcer know directly if they wish to be excluded. Remember to keep a note of the announcement.
* Whilst it is not illegal to take pictures in public places and use them online it is not recommended as it is impossible to know if this will cause individual upset to residents.
* Try and use images that do not make it possible to easily identify an individual or use images from online brokers where permission to use has already been granted. Never use images of children without express permission.

In addition to the above guidance consideration must be given to:

* + Getting permission in writing if we will retain and use the image for promotional purposes.
  + Ensuring that adequate data sharing routines are in place to prohibit inappropriate sharing of the image (please refer to GDPR guidelines).
  + Minimising the time images remain on unsecured devices such as cameras, to limit the chances of the image being transferred or used inappropriately.
  + Establishing good working practises & procedures with devices to minimise risk of theft of device containing pictures which could be used outside of the Council.

Safety when using ICT equipment

* 1. Employees must not use hand-held equipment while driving. This is illegal under UK law and dangerous.
  2. Employees must park their car and switch off the engine to use a hand-held piece of equipment while in the car. It is illegal for the engine to be running while using a mobile device.
  3. The Council recommends that staff DO NOT conduct business calls while driving due to the risk of distraction. Staff taking business calls on a car-kit must self-assess the risk of distraction (considering the nature of the call, call duration, and the traffic conditions) and terminate the call where appropriate.
  4. Please be aware that you are never obliged to take a work call whilst driving.

Please ensure that you always use ICT equipment in accordance with specific recommendations as per the Council’s Safety Policy and applicable health & safety guidance.

Physical Security

Identification of Staff

Physical or traditional security is equally important to the overall security of the ICT environment, working in parallel with the ICT security products.

It is very important that we can:

* + 1. Identify electronically and physically the users of our systems
    2. Ensure that the environment is not physically tampered with, to either disrupt services or bypass technical controls.

To achieve this, it is important that the following controls are followed:

* + 1. All Council staff must wear their Council always supplied ID badge.
    2. To safely identify staff, on joining the Council staff must supply a head and shoulders picture of themselves to the council. This will be used for Creation of the Staff ID badge, loading onto the Staff Telephone Directory, Loading on the ICT Domain Directory
    3. Observe the “last person out” routine (See Appendix F) and check your area as you leave ensuring that cupboard doors and windows are locked as you exit.
    4. If ICT equipment has been left unattended in the office, please hand equipment back to either ICT or HR. ICT or HR will identify the owner of the equipment and arrange for its return.
    5. If you see anyone accessing the Network cabinets or Computer room and they are not accompanied by a member of the ICT team, then please report this to ICT immediately.

Identification of Visitors

It is also very important that we can easily identify visitors so that personal information is not inappropriately disclosed.

When you have a visitor in your area, please observe the following guidelines

* + 1. Reception must be advised of the name of all visitors and have a contact number to notify when the visitors arrive.
    2. You are responsible for ensuring your visitors always wear the yellow visitor’s lanyard.
    3. Do not leave visitors unattended in the general office space; try and locate a visitor in an office/meeting room to work wherever possible.
    4. Introduce your visitor to your colleagues to ensure that any confidential material or discussion is not accidently seen, appropriated, or overheard.

Computer Room

The following access conditions apply to the Civic Centre Computer room which is under the control of the ICT team.

* + 1. Non-ICT staff must never attempt to access the Computer Room. Doing so may be considered a serious matter and subject to disciplinary action.
    2. The room must be always locked when unoccupied.
    3. Please be aware that CCTV is in place to monitor access.
    4. Only authorised staff have access to the room.
    5. Staff wishing to have access to this room may do so only with permission of the ICT manager and must be always accompanied by a member of the ICT team.
    6. The room must be always left free from clutter.
    7. Paper, cardboard, and other combustible products must be removed from the room as soon as practically possible after use.
    8. Drinks or food must not be taken into the room at any time.

Network Equipment and Cabinets

The following access conditions apply to the network cabinets in all buildings in the St Albans estate, which are under the control of the ICT team:

* + 1. Non-ICT staff must never attempt to access the network cabinets or tamper/disturb network equipment. Doing so may be considered a serious matter and subject to disciplinary action.
    2. The Network cabinets must be kept always locked. Only authorised ICT staff and ICT approved contractors must access the cabinets
    3. Non-Authorised Staff must not
    4. Move/Add/Remove cables within the cabinets
    5. Make any attempt to connect to the network switches
    6. Plug any equipment directly into the network switches
    7. Network equipment must always be in a secure, locked network cabinet.

Network Security

The management and control of the Council’s network is the responsibility of the ICT department.

External connections in and out of the Council’s network are subject to controls that protect our network, and more importantly the data processes and stored on the network.

Anyone requiring an external connection, either for support of services or business activity must contact the ICT department.

Use of collaboration tools for sharing desktops with 3rd parties for support purposes must be carefully controlled to avoid malicious or accidental loss of data.

(Please see our guidance on Collaboration Safety for more information).

Likewise, use of data sharing tools such as Dropbox must be carefully controlled, and users must seek authorisation from the ICT desk before sharing data via these methods. We recommend using SharePoint.

Storage

To maintain the confidentiality and integrity of our data, access to files will only be authorised to those who require the data as part of their normal duties.

The Council’s ICT Service will grant access to individual data areas as requested in writing by the “owners” of that area.

Additionally, managers and supervisors will have access to their staff’s individual working areas if required.

It is expected that users will make all files of general interest available (normally read only) on a suitable location on the server(s), or on the intranet.

Each user is assigned an individual storage area, known as your Personal P:/ drive or OneDrive. Only you have access to the files in this area unless you specifically ask the ICT Service Desk to grant access to others (which is not recommended).

Please note – the provision of storage is for the council business use only. It is not permitted to store personal information and media on these services which includes photographs and music.

Uploading Policy

Any person uploading information must be sure that the information being uploaded is suitable to upload, and not confidential or personal.

Do not post anything on the Internet that could be seen to represent the Council or repeat information you are aware of through your work at the council unless you are authorised to do so.

If information is confidential or person-specific, advice must be sought from the ICT Service Desk to ensure security controls are in place. Care must be taken when using cloud-based services to ensure data is European Economic Area hosted and in accordance with Data Protection Act requirements.

Download Policy

Individuals may need to download information including PDFs and Microsoft Office files from the Internet. To reduce the likelihood of a virus infection, individuals must take care to ensure that the files are from a trustworthy source.

Graphical, audio and video files may be downloaded and stored on the council’s network for business use only. Individuals with personal needs for accessing such files must use their own personal equipment and internet connections to do so.

Individuals requiring any new software, including any plug-ins, must make a formal request to the ICT Service Desk (Ext 6999).

Reminder: Software must not be downloaded and/or installed onto Council ICT equipment unless

* It has been approved by the Corporate ICT Service.
* The license can be validated that it is licensed for current use.

Copyright laws apply to the internet and care must be taken when re-using any information (including images) in any Council work. If there is any doubt, individuals must liaise with St Albans Legal Services department.

ICT Asset Management

Procurement & Asset Management

* + 1. All procurement of equipment, software, infrastructure, and services to be used on behalf of the Council, must be procured with the agreement of the St Albans ICT Team.
    2. All assets which are considered not to be consumables, will have an ICT asset tag attached to it, and will be entered in the St Albans Configuration Management Data Base (CMDB) which is held in Salesforce.
    3. If a department wishes to permanently move an asset either to another staff member, or between departments they must notify the ICT team so the CMDB can be modified.
    4. If a member of staff leaves the organisation, the ICT asset must be returned to the ICT team.
    5. If a member of staff goes on maternity or is on long term sick (28 days), the ICT asset must be returned to the ICT team and reimaged.
    6. Managers are not permitted to hold onto equipment or keep spare equipment as this prevents an efficient use of equipment and poses an ongoing security risk to the Council. All returned devices will be rebuilt, cleaned, and re-issued. This ensures that the Council makes the most effective use of its ICT estate.

Unless the equipment is part of a new post business case, managers will not be required to repurchase the kit, when next required.

Disposal and Reuse of ICT equipment

The ICT Team must be consulted over the reuse of IT equipment and will advise

on removing any information held on the equipment.

Disposal of redundant equipment is the responsibility of the IT Department. Anyone disposing of redundant computer equipment such as monitors, workstations,

keyboards, printers, etc., must contact the IT service desk to arrange for collection and

disposal in accordance with the WEEE regulations.

Line managers must ensure that such equipment is not:

* + 1. Transferred outside of the Council.
    2. Sold or donated to charitable organisations without prior approval from the St Albans ICT Department.
    3. Equipment loaned for any period to a 3rd party without the express permission of the ICT team and ensure that the device has been wiped appropriately.

3rd Party Supplier Management

System owners are responsible for the management of 3rd party suppliers

The following guidelines must be followed by system owners

* 1. Partner agencies or 3rd party suppliers must not be given details of how to access the Council’s network without a signed business case from ICT approving them to have access.
  2. The 3rd Party being granted access must sign the 3rd Party acceptable use policy before being granted access.
  3. Partners or 3rd party suppliers must contact the IT service desk every time before connecting to the St Albans District Council network and not be granted permanent access.
  4. Informing the ICT services desk of 3rd party staff leaving their employment so that their accounts can be disabled.
  5. Notifying ICT of long-term absences regarding a 3rd party (3 months or longer) so that accounts can be disabled appropriately.

Change Control

All proposed changes to the Council’s ICT infrastructure and services (e.g. software

upgrades/installations and new IT services) must gain approval of the IT Change

Advisory Board (CAB) before implementation.

This procedure is necessary to ensure that changes are feasible, desirable, implemented with the minimum of disruption to Council services. Any department envisaging a change and/or planning upgrades and modifications must contact the IT Service Desk to initiate a change to the infrastructure/service. This is known as a Request for Change (RfC).

PCI DSS

Credit card data stored, processed, or transmitted by the Council must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

Staff involved in taking and processing payments must conform to the responsibilities as set out in the separate ICT PCI DSS Personal Commitment Policy.

Sensitive credit card data is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

It is the responsibility of the Council to publish and disseminate PCI DSS policy and instructions to all relevant users (including staff, vendors, contractors, and business partners).

The Council must, ensure this section is reviewed and updated against changing PCI DSS regulation updates as issued from time to time, or when there have been significant risk changes to the operational business environment to ensure continued compliance with PCI DSS regulations.

All users who handle PCI data must conform to the standards set out in the PCI-DSS Security Standards.

Human Resources Information Security Standards

Our staff and partners are vitally important to the overall security of the environment. To minimise the threat from malicious, or accidental behaviour that could impact on the availability, confidentiality or integrity of data, the following controls are enforced when staff join our organisation.

The Council will carry out “Baseline Personnel Security Standard” (BPSS) checks on all new entrants to ensure that they are authorised to access the Council information systems.

Every Line Manager is responsible for

* 1. Ensuring that all their staff are trained to use information systems securely.
  2. Ensuring that all their staff have read and signed this policy.
  3. Ensuring that all staff complete their annual mandatory cyber training.
  4. Ensuring that user access to information systems is removed promptly when the requirement for access ends.

Legal Responsibilities

The Council will ensure that every user is aware of, and understands, their responsibilities under the UK General Data Protection Regulations (GDPR)and Data Protection Act 2018 or any other relevant legislation.

The Council will ensure compliance with:

* + - Data Protection Act 2018.
    - UK GDPR
    - Law Enforcement Directive (LED)

Privacy and Electronic Communications Regulations (PECR)

Every Council Officer has a duty to provide advice and assistance to anyone requesting information under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004, as well as the access rights under the UK GDPR and DPA 2018.

Legislation

The Council must abide by all relevant UK and EU legislation.

This policy is based on industry good practice and complies with:-

* Government Connect Secure Extranet Code of Connection (CoCo).
* Data Protection Act 2018
* UK General Data Protection Regulation
* Computer Misuse Act 1990
* Freedom of Information Act 2000
* Environment Information Regulations 2004
* Health & Safety at Work Act 1974
* Human Rights Act 1998
* Regulation of Investigatory Powers Act 2000

In addition to the above legislative controls, all staff must be aware of and comply with the following Council policies and procedures.

* + GovConnect Personal Declaration Form.
  + Homeworking Policy and Procedure.
  + Responsible Reporting (Whistle Blowing) Policy.
  + Guidelines for Managers & Supervisors – IT Incident Reporting & Requesting Data about Email & Internet Usage
  + Guidelines on Best Working Practices in the Use of the Councils IT Systems and Devices, Including the use of E-Mail and the Internet.
  + All FOI, EIR and GDPR policies and procedures

Communications and Operation Management

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

The key principles staff must be aware of with the management of the ICT service are set out below:

* 1. Changes to the Council’s operating systems must follow the Council’s formal change control procedure. Only authorised changes will be made to the Council ICT service (including any information systems and information processing equipment) and will follow a formal Change Management process. Changes can be requested by submitting a Change form.
  2. Un-patchable software must not be used when out of support life. It is the responsibility of the System Owner to track the end of support dates for their application and plan with involvement from the ICT team upgrades. (Please note: The service must make financial provision to undertake a major upgrade at least every 2 years).
  3. Appropriate access controls have been put in place to prevent user installation of software and to protect against malicious and mobile code. Users must not attempt to circumvent these controls.
  4. Regular backups of essential business information are taken to ensure that the Council can recover from a disaster, media failure or error.
  5. Storage media must be handled and protected with care.
  6. Disposal of storage media must only be undertaken by ICT.
  7. ICT retain relevant audit logs in line with legislation.
  8. Connections to the Council network are made in a controlled manner.
  9. An annual health check will be made of all Council IT infrastructure systems. Departments may be required to make technical changes to their application environment to remain in PSN Compliance, and departments must hold contingency funds to cover this.

Policy Compliance

If any ICT user is found to have breached this policy, they may be subject to St Albans City and 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 your line manager in the first instance.

Policy Governance

The following table identifies who within the 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 people or groups to be consulted prior to final policy implementation or amendment.

Informed – the people or groups to be informed after policy implementation or amendment.

|  |  |  |
| --- | --- | --- |
| **Area** | **Role** | **Named Contact** |
| Responsible | Strategic Director – Customer, Business and Corporate Support | Suzanne Jones |
| Accountable | IT Manager | Leon Thomas |
| Consulted | UNISON;SLT | Amanda Foley  Suzanne Jones  Dale Phillipson  Chris Trail |
| Informed | All Council Employees, All Temporary Staff, All Contractors. | Various |

Business Continuity Planning

The Council’s BCP is designed to counteract interruption to business activities and to protect critical business processes from the effects of major failures or disasters.

The Corporate Service Recovery Plan details the Council’s process for managing business continuity across the organisation. The plan is owned and maintained by the Risk Management Group.

The ICT Sections of the plan describe the procedure for reacting to a disaster and recovery of systems, including invocation of the disaster recovery contract with DAISY.

Testing of the ICT disaster recovery procedures take place annually. The aim is to test the recovery procedures for all application every 5 years. Departments will be asked once every 5 years to take part in the disaster recovery test.

Review and Revision

This policy will be reviewed in line with legislation changes, business changes and as it is deemed appropriate, but no less frequently than every two years.

Policy review will be undertaken by the ICT team.

Appendix A - Constraints on using GSCX mail and Personal Commitment Statement

What are PSN users?

PSN users are those staff who:

* + Have access to PSN services such as the Government Gateway and the DWP Customer Information System

The Baseline Personnel Security Standard

In order to gain PSN compliance the Council must demonstrate that it complies with the requirements of the Baseline Personnel Security Standard (BPSS). BPSS is the minimum standard required to ensure the identity and integrity of an employee with access to official information. It involves four main elements:

* + Identity Check
  + Nationality and Immigration Status
  + Employment history (past 3 years)
  + Verification of Criminal Record (unspent convictions only)

Full details of the BPSS can be found here: <https://www.gov.uk/government/publications/security-policy-framework>.

GovConnect Personal Declaration Form

GovConnect Personal Declaration Form

Please read the following statements carefully and complete the personal declaration:

* I accept that my use of Government Connect may be monitored and/or recorded for lawful purposes
* I accept that communications sent or received by means of Government Connect may be intercepted or monitored
* I will make myself familiar with the security policies, procedures and any special instructions that relate to Government Connect and be aware of the impact of loss of any material and the actions to take in the event of any loss. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant.
* I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via Government Connect as appropriate and will not send Protectively Marked information over public networks such as the internet. I will always check that the email addresses on recipients’ email messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain.
* If I use St. Albans City and District Council mobile services from outside the United Kingdom, I will contact the ICT Service Desk for advice and to be aware of the risks of using IT equipment overseas.
* I will not auto-forward from my Government Connect account to any other email account.
* If I am about to leave St. Albans City and District Council, I will inform my manager prior to departure of any important information held in my account.
* I do not have any unspent criminal convictions (for further information on this, see guidance overleaf).

|  |  |
| --- | --- |
| Employee signature: |  |
| Printed name: |  |
| Date signed: |  |

BPSS compliance

Responsibility for BPSS compliance lies with the HR Team. They will ensure that all PSN users) have signed the GovConnect Personal Declaration Form (see section 25.4) prior to using PSN-related IT services.

* + They will also ensure that these staff have been subject to a Basic Disclosure check at the point of recruitment and at three-yearly intervals thereafter.
  + A decision is pending about a potential requirement to obtain a 10-year employment history for PSN users.

Incoming emails to email accounts

Incoming e-mails must not be forwarded or copied to any non-work accounts. This prohibition applies equally to Council staff, Members, and all external email accounts such as Google, Yahoo and Microsoft.

Documents or files that are attached to emails can be stored with the email inside the email account. However, it is good practice to store such attachments in a shared space where other members of the team can search, retrieve, and view them. Where this occurs, the attachment must be stored in a secure team “space” such as:

* + A software application e.g. as Orchard Housing
  + A document management system such as Civica
  + A secure shared network folder.

Appendix B – Password Policy

The password policy is:

* + Password must be 9 characters minimum in length
  + Password must contain 3 non-connected words (CoffeeFishdogma) for example, or a random set of characters rather than dictionary words
  + Password must contain a mixture of LowerCase, UpperCase, numbers and symbols ideally with the special characters, rather than simply an exclamation mark

*Note: You are trying to make it difficult for someone to try and break the password: Putting numbers and symbols throughout the password improves password strength, rather than just at the end which is commonly used. (see example below)*

.

**Beware of social media:**

* If someone is targeting you, they may look at your social media presence to see what you are interested in. If you like dogs for example, don’t include anything about dogs in your password
* Beware of social media quiz’s – they might be fun, but you are handing over information that hackers may use against you. Let’s face it – do you really know who has access to your quiz answers when you do them online?

**Do not re-use passwords**

* Never use passwords that you use at work outside of the work environment
* Keep your password you use to log onto your computer **completely** different from passwords that you use to log into any applications.
* Make sure any application passwords are as complex as your computer password – especially if the application is hosted (e.g Jigsaw)

**What makes a poor password choice?**

* + Passwords where it is the first set of keys on the keyboard either vertically or horizontally are very weak as it is a combination of characters that is replicated on millions of keyboards across the world and is probably the first type of password crack that would be tried in the event of a proper attack.
  + Passwords using days of the week
  + Passwords using Names, especially famous people’s names.
  + Passwords using Pet Names
  + Passwords using Place Names
  + Avoid swapping out common letters for symbols such as @ for a’s, 1 for I’s or L;s, 0 for o’s etc as these are easily guessable

Example

|  |  |
| --- | --- |
| Weak | Strong |
| GeenLettuce123 | Tetchy$lettuce^dogma287 |

**Appendix C – E-Mail signature formats**

Regards

**Firstname Surname**

Job Title

Department

**St Albans City and District Council**

Direct:  01727 81xxxx Ext xxx

Mobile: xxxxx xxxxxx

Council general home page:              [www.stalbans.gov.uk](http://www.stalbans.gov.uk/)

Council contact details and address: [www.stalbans.gov.uk/contact-us](http://www.stalbans.gov.uk/contact-us)

Note: When communicating to the general public- please ensure that you have an e-mail footer than omits your personal phone number. Please see guidance from your manager where appropriate.

**g**

Appendix D - E-Mail Out of Office Template

Out of Office Email template:

A standard out of office template must also be used by all staff as follows:

Thank you for your email I am out of the office until [dd/mm/yy]. If you have an urgent enquiry please contact [full name, job title] at [email address] or telephone them on [telephone number].

Kind Regards

**Firstname Surname**

Job Title

Department

**St Albans City and District Council**

Direct:  01727 81xxxx Ext xxx

Mobile: xxxxx xxxxxx

Council general home page:              [www.stalbans.gov.uk](http://www.stalbans.gov.uk/)

Council contact details and address: [www.stalbans.gov.uk/contact-us](http://www.stalbans.gov.uk/contact-us)

Or if relevant to the work you do, direct people to specific members of staff e.g. If you have an urgent enquiry regarding refuse collection please contact [full name, job title] at [email address] or telephone them on [telephone number]. . If you have an urgent enquiry regarding licensing please contact [full name, job title] at [email address] or telephone them on [telephone number].

Appendix E – How to send encrypted e-mail

The mechanism to send secure mail is Zivver. Find below the instructions on how to use Zivver

<https://stalbanscdc.sharepoint.com/sites/StaffNet/SitePages/Zivver(1).aspx>

Appendix F: Last Person Out routine

The last person out routine is an informal office protocol that requests that the last person to leave the office area they work of an evening, performs a quick scan of the area to ensure that no equipment and/or paperwork has been accidentally left in a insecure manner. Should they detect that that has happened, the officer should secure such material, and leave a note on the desk advising how to retrieve the material.

This also applies to ensuring that ground floor/accessible windows are also shut and that no doors have been left open in appropriately.

Appendix G: Reporting a lost phone

Find below the procedure for reporting damage, loss, or a stolen phone immediately to the IT Team (01727 819587) during office hours or directly to the mobile network Vodafone (Tel: 03333 043333) outside of normal office hours.

Appendix H: Data categorisation

What is personal data?

The UK GDPR defines ***personal data*** as: “any information relating to an identified or identifiable natural person (‘data subject’)”. This means that any information that identifies, directly or indirectly, an individual, whether by reference to their name, or an identification number, or location data such as an address, or an online identifier, or “one or more factors specific to the physical, physiological , genetic, mental, economic, cultural or social identity of that natural person….” will be personal data (Article 4)

This will include any expression of opinion about individuals or indication of the intentions of us or others in respect of that individual, for example, comments made about an individual in an email exchange.

For the purposes of the UK GDPR, processing personal data includes “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure (by any means)…. making available, alignment or combination, restriction erasure or destruction…”(Article 4)

For us this means whenever you obtain and then use personal data it will be processing for the purposes of the UK GDPR. It will continue to be processing until it is deleted. This includes personal data held as an archived record.

What is special category personal data and/or criminal convictions data??

**Special category personal data** means information about an identifiable individual relating to their:

* + Racial or ethnic origin
  + Political opinions
  + Religious or philosophical beliefs
  + Membership of trade union
  + Genetic data or biometric data (processed for the purposes of identifying an individual)
  + Physical or mental health
  + Sex life or sexual orientation

Special category personal data cannot be processed unless we can comply with certain criteria in Article 9 of the UK GDPR.

The use of data relating to **criminal convictions**, which includes information about convictions, offences, proceedings, and allegations relating to offences, ialso requires us to comply with certain criteria in the DPA 2018 and the LED.

Individuals are less likely to want special category data and criminal convictions data shared and therefore the UK GDPR and DPA require additional criteria to be complied with when handling these types of data.. .