#

# N:\10.Implementation\WS1-FrontDoor\Brand\Image-AdoptionWest.PNG

# ICT Security and Acceptable Use Policy

### Version history

|  |  |  |
| --- | --- | --- |
| **Version**  | **Date**  | **Amendments**  |
| **1**  | October 2018  | v.1  |
| **2**  | October 2019 | v.2 |
| **3**  | October 2020 | v.3 |
| **4** | October 2021 | v.4 |

Date of next review: October 2022

Electronic Copies

An electronic version of this document is available at [www.adoptionwest.co.uk](http://www.adoptionwest.co.uk)

### Comments and Suggestions

We welcome comments and suggestions from readers. They will help us to improve this document in later editions. Please make them to info@adoptionwest.co.uk

## Contents

Contents

[ICT Security and Acceptable Use Policy 1](#_Toc498933974)

[Version history 1](#_Toc498933976)

[Comments and Suggestions 1](#_Toc498933978)

[Contents 2](#_Toc498933979)

[1 Introduction 4](#_Toc498933980)

[1.1 Welcome to the ICT Security and Acceptable Use policy 4](#_Toc498933981)

[1.2 Why focus on the security and acceptable use of ICT? 6](#_Toc498933982)

[2 Scope 8](#_Toc498933983)

[3 Terms and definitions 8](#_Toc498933984)

[4 Organisational security 8](#_Toc498933985)

[4.1 Responsibilities 8](#_Toc498933986)

[4.2 Contractors 9](#_Toc498933987)

[5 Asset classification and control 9](#_Toc498933988)

[5.1 Inventory of assets 9](#_Toc498933989)

[5.2 Information classification 10](#_Toc498933990)

[6 Personnel security 10](#_Toc498933991)

[6.1 Training 10](#_Toc498933992)

[6.2 Responding to security incidents 11](#_Toc498933993)

[7 Physical and environmental security 11](#_Toc498933994)

[7.1 Secure areas 11](#_Toc498933995)

[7.2 Equipment security 11](#_Toc498933996)

[7.3 Security of equipment off-premises 12](#_Toc498933997)

[7.4 Portable devices 13](#_Toc498933998)

[8 Communications and operations management 13](#_Toc498933999)

[8.1 Unauthorised Software 13](#_Toc498934000)

[8.2 ICT Security and Acceptable Use Monitoring 14](#_Toc498934001)

[8.3 Backups 14](#_Toc498934002)

[8.4 Archiving information 14](#_Toc498934003)

[8.5 The Internet and Cloud Services 14](#_Toc498934004)

[8.6 Email 15](#_Toc498934005)

[8.7 Computer viruses 16](#_Toc498934006)

[8.8 Phishing emails 17](#_Toc498934007)

[9 Access Control 18](#_Toc498934008)

[9.1 User access management 18](#_Toc498934009)

[9.2 Screensavers 18](#_Toc498934010)

[9.3 Modems and other network connectivity 18](#_Toc498934011)

[9.4 Passwords 19](#_Toc498934012)

[9.5 Remote control software 20](#_Toc498934013)

[9.6 Connection to Adoption West’s data network 20](#_Toc498934014)

[10 Business continuity management 20](#_Toc498934015)

[11 Compliance 20](#_Toc498934016)

[11.1 Computer Misuse Act 20](#_Toc498934017)

[11.2 The Data Protection Act 21](#_Toc498934018)

[11.2 Caldicott Guardian 21](#_Toc498934019)

[11.3 Intellectual Property Rights 21](#_Toc498934020)

[11.4 Software copyright 21](#_Toc498934021)

[11.5 Unauthorised use of equipment 21](#_Toc498934022)

[11.6 System Audits 21](#_Toc498934023)

[11.7 Compliance testing 21](#_Toc498934024)

[12 Miscellaneous 22](#_Toc498934025)

[12.1 Waste disposal 22](#_Toc498934026)

[12.2 Accidental verbal disclosure of information 22](#_Toc498934027)

[Annex A - Staff Quick Security Guide 23](#_Toc498934028)

# 1 Introduction

## 1.1 Welcome to the ICT Security and Acceptable Use policy

ICT security and the acceptable use of Adoption West ICT resources is essential to protect the organisation’s information, data, staff and reputation as well as its investment in hardware and software. It also reduces the risks of fraud and inappropriate access to confidential organisation data and services, such as the Public Services Network (PSN).

There has been a phenomenal rise in cyberattacks over the last few years with large organisation losing vast amounts of data or suffering other serious breaches.



One form of cyberattack called ransomware has seen explosive growth and presents a serious risk to many organisations.



It is only through diligence and following processes and procedures that the risk of systems being compromised can be mitigated, and potentially catastrophic loss of the ability to function as a business, financial loss and reputational damage be avoided.

**Everyone who uses the organisation’s ICT systems and equipment must read, understand and comply with this Policy. Observing this policy is a formal requirement for all staff and users of the organisation’s ICT systems. Failure to follow this policy will be fully investigated as a serious incident requiring investigation and could result in disciplinary and/or legal action being taken against the individual(s) concerned resulting in dismissal and/or criminal proceedings. Legal action can include the recovery of costs or damages incurred by the organisation due to the actions of users. You should refer to the employee code of conduct for further information.**

Every ICT user must take security issues seriously. Even if you consider yourself an occasional or unsophisticated user, you could be the channel by which a virus is introduced, a hacker gains access to our systems or we are in contravention of an Act.

Everyone responsible for using personal data has to follow strict rules called ‘data protection principles’. They must make sure the information is:

* used fairly, lawfully and transparently
* used for specified, explicit purposes
* used in a way that is adequate, relevant and limited to only what is necessary
* accurate and, where necessary, kept up to date
* kept for no longer than is necessary
* handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Further information about the Data Protection Act and other legislation can be found on the gov.uk website e.g. <https://www.gov.uk/data-protection/the-data-protection-act>

**A data breach could lead to Adoption West being reported to the Information Commissioners Office (ICO) or via the NHS information governance toolkit. For Adoption West this could mean reputational damage and/or fines of up to £500,000. In the future, that amount could be increased under GDPR to €20m.**

This policy is designed to make ICT fully available to anyone in a safe and secure way.

The policy has been written in non-technical terms and covers the essentials that all users need to know and comply with. Staff with a specialist ICT role or responsibility should also read the ICT Security Processes and Practices document.

## 1.2 Why focus on the security and acceptable use of ICT?

It is important to everyone. Think about your own car or bank account. You would not:

* leave your car unlocked and the keys in the ignition
* fill your car with what seems like fuel which you happened across on the street
* tell a complete stranger in the street your home address and give them your keys
* write your PIN on your credit card

Yet surprisingly some people do very similar things when it comes to ICT systems; writing passwords on Post-It notes near their computer, letting colleagues log in as you, loading untested software, and many similar practices are equally risky. There is more information about passwords, for example, in Section 9.4.

This policy gives guidance for safe and secure use of ICT systems. It’s a list of basic, good housekeeping that everyone must observe.

Where appropriate we have tried to explain why these requirements exist. But the risks are so many and diverse that we can’t cover them all.

For example, most people have heard of viruses and understand that they can cause a great deal of damage and inconvenience. But there are other risks, such as hidden bits of software that secretly record all your keystrokes and then send them to an unknown third party allowing them to access systems with your details.

Commonplace use of the internet, wireless communication, mobile devices and ‘cloud’ services have changed the boundaries of ICT systems. No longer do the physical walls and doors of the organisation’s offices protect them. Malicious people can attack from anywhere in the world, and information you might think harmless or trivial can be a key advantage that they can exploit. Social Media, Facebook, Twitter or LinkedIn for example, are examples of where hackers gain useful information in this way. Avoid posting details that you would not give to a stranger and remember once your information is out, it cannot really be retrieved or withdrawn.

Adoption West relies on its data network to not only access but also to secure and protect its information assets. But the devices you use to carry out your role can also be used maliciously if they fall into the wrong hands. You may not realise how much damage a skilled person could do from your device or information – so don’t let them.

# 2 Scope

This policy applies to all individuals and/or organisations that access Adoption West’s ICT systems, software, data and network as well as authorised, connected networks and services. This includes:

1. all staff, including part-time, temporary staff, individual contractors and agency workers;
2. board members;
3. partner organisations with access to the ICT network and systems;
4. contractors with access to the ICT network and systems.

# 3 Terms and definitions

**Information Security** **(IS)**

Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

**Information Governance (IG)**

The structures, policies and practice of the organisation and its partners to ensure the confidentiality and security of all records, and to enable the ethical use of them within the law for the benefit of individual citizens.

More information about IG policies can be found at[**www.adoptionwest.co.uk**](http://www.adoptionwest.co.uk)

**Acceptable Use**

Standards for the behaviour of personnel using Adoption West’s ICT resources and authorised networks and services, whether on or off site.

# 4 Organisational security

## 4.1 Responsibilities

The Service Director has overall responsibility for the maintenance and management of this policy working closely with our ICT provider. The policy is an integral part of the information governance framework.

The management team meet regularly with the ICT provider to deal solely with ICT security and also consider any technical changes or projects.

Internal Audit review this policy as part of their standard auditing cycle.

**Every manager and member of staff is responsible for operating and enforcing this policy. In most cases when you log in to the network you are asked to reaffirm your understanding of the policy and therefore you should re- familiarise yourself with the document(s) from time to time.**

## 4.2 Contractors

Contractors can only be used for support or given access to systems or data if they have agreed to comply with this security policy. Any requests for quotes or tenders for ICT systems or services need to include this policy and the ICT Security Processes and Practices document and the resulting contracts ICT must include signed agreement to it. The appropriate form can be obtained from the ICT provider service desk.

Visitors to premises, including suppliers and consultants working on-site, should never connect their own devices to our network via WiFi or a wired network connection. The only exception is Guest WiFi. If full access to the network is required, a managed device and appropriate/minimal credentials for the task they need to complete should be applied for via the ICT provider service desk.

# 5 Asset classification and control

## 5.1 Inventory of assets

The following is an example of the sort of equipment owned by Adoption West which is recorded on the ICT inventory:

* any infrastructure devices (such as servers and switches)
* thin client devices
* desktop devices
* laptop devices
* tablet devices
* smartphones, other types of mobile phones, SIM cards and 3G dongles
* handheld computing devices
* mobile storage devices (including USB drives or anything that stores data)
* monitors, scanners and projectors
* printers and plotters
* dial-up modems

The list of items to be included in the inventory may be extended from time to time.

Whilst ICT record details about the device itself, it is the responsibility of managers to track and record who has use of equipment at any one time. Ultimate responsibility for loss of equipment resides with the manager of the people using the equipment.

It is the responsibility of managers to ensure that equipment is held securely. When staff leave Adoption West and the vacant post is then filled the equipment must be reallocated to the new post holder. Before reallocation or reuse, the device must be returned to IT to be re-imaged and have the latest updates installed.

However, when the post is not going to be filled or is deleted managers must ensure that any surplus equipment is either returned to IT for recycling if near end of life or reused to replace the oldest equipment. Equipment must not be stored locally for longer than necessary because it is considered an organisational asset that can be reused elsewhere, saving Adoption West valuable resources. When a unit of equipment is reallocated Managers must inform ICT so that they can maintain their records.

**Importantly, any equipment which is stored locally by staff may be forgotten about and poses a security threat as it is not regularly patched and its data will not have been destroyed in a compliant manner. For this reason devices which have not been connected to the network for 60 days will be disabled.**

## 5.2 Information classification

Information classifications are official, secret and top secret. Adoption West will use the official classification to protectively mark information so that it is recognised and treated as being more sensitive. Adoption West uses the official marking for sensitive information such as personal data, and unmarked for other general information that does not need any special protection such as that published on the public facing website.

The loss of information can result in adverse incident reports which will not only affect the reputation of Adoption West but, in the case of disclosing personal information intentionally or recklessly, it is also a criminal offence.

Adoption West maintains an Information Asset Register which is also be used to record the classification of information.

# 6 Personnel security

## 6.1 Training

All new ICT users will be provided with electronic access to this security policy as part of their induction. Before a network login is given to a new starter they will have to confirm their acceptance of the ICT security policy and undertake an online training module. The assessment associated with the new ICT Security & Information Sharing e-learning module will have to be passed when required in order to gain a network login.

All staff will also have to complete refresher training on an annual basis. If the annual refresher training is not successfully completed, access to network and services will be removed until confirmed as complete.

All users are required to confirm their acceptance of the ICT Security Policy every time they start-up and log onto their computer.

People from other organisations (partners or suppliers) who need to use Adoption West’s ICT network and systems will be required to confirm their agreement to comply with the policy in writing and complete the online training or demonstrate equivalent knowledge e.g. through the agreed contract before network access is granted. Should the related online assessment not be passed, access will be disabled. Additionally, a ‘sponsoring’ senior manager of Adoption West will be required to confirm that this access is necessary and the individuals concerned are suitable people to be given this access. A form for this purpose is available from the ICT helpdesk.

## 6.2 Responding to security incidents

If you are aware of or suspect any action that is contrary to this policy you must report it as soon as possible by reporting it to your manager or a member of the management team. You should also refer to Adoption West’s data breach policy which covers both electronic and non-electronic data breaches and reporting incidents to the following: info@adoptionwest.co.uk.

# 7 Physical and environmental security

## 7.1 Secure areas

Under this policy certain areas are designated as **secure areas** because of the equipment or type of data held within them. These areas will be clearly signposted, and have controlled access.

Staff who work in or have access to a **secure area** should ensure they comply with guidance for working in such an area and also read the ICT Security Processes and Practices document.

## 7.2 Equipment security

Equipment should be located as securely as possible, so as to minimise the risk of potential threats, including but not limited to:

* malicious electronic activity
* theft
* fire
* smoke
* water
* dust
* vibration
* electrical supply interference
* vandalism

Staff deciding to leave their portable/mobile ICT equipment in Adoption West premises overnight, or at the weekend, should ensure that it is locked away out of sight. Failing to do this leaves the equipment vulnerable to theft and so could lead to disciplinary action being taken if the device is stolen.

Special attention should be paid to equipment in public areas to prevent interference or loss.

Additionally, equipment in public areas or sited next to windows must be checked to prevent the risk of overlooking whilst in use. Blinds should be closed at the end of the day to reduce the risk of theft.

If you see a person you do not recognise to be a member of staff entering Adoption West / council premises and they are not displaying an Adoption West / council identification badge, report their presence to your line manager. Please be aware of who is following you through security doors to prevent unauthorised access to the building. Any suspicious activity should be reported.

Team managers should ensure all their staff wear identification which clearly displays their picture and name at all times whilst in work premises.

## 7.3 Security of equipment off-premises

Special consideration must be given to equipment and media taken off work premises. Does the equipment really need to be taken off the premises? If it is a meeting, could it be conducted via Skype or conference call?

Although not strictly ICT, note that printed material is even more risky than equipment as it cannot be encrypted, so it should not be used as an alternative to taking equipment.

If the equipment must be taken, then for example it must:

* not be left unattended in public places
* not be left in an unattended vehicle (unless the risk of carrying it is greater, in which case it should be locked away out of sight for the minimum amount of time, and must not be left there overnight). For this situation, the device must be:
1. Encrypted. All laptops should be encrypted by default but if ICT have informed you that there are issues or there is any doubt with this then laptops should not be removed from work premises.
2. Powered down (not just locked or suspended – this is to prevent possible overheating or detection due to audible alerts).
3. Kept separate from your work phone – not in the car with your laptop.
4. On no account should your username and password be written down and kept with your laptop.
* be carried as hand luggage and disguised when travelling
* not be taken abroad (unless authorised in writing by the Business Manager or Service Director)

For further information you should refer to the home working policy.

Also, please see section 8.5 regarding how to access the network off-premises to store and retrieve documents etc.

Typical manufacturers’ instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields, extremely high or low temperatures, humidity/water ingress, impact, vibration, dust/sand etc.

## 7.4 Portable devices

Particular care should be taken to ensure the safe custody of portable devices. This covers:

* laptops
* tablet devices
* smartphones
* other mobile phones
* other handheld devices
* mobile storage devices, including any type of USB drive or anything that stores data

Where appropriate devices are encrypted to ensure no Adoption West data can be accessed by non-Adoption West staff in the event of a loss, but of course this will not deter theft as the thief is most likely interested in the equipment rather than the data.

It should be noted that SD cards for use in cameras cannot be encrypted and so extra special care should be taken to ensure safe custody of this kind of storage device, and secure erasure when the data is no longer required. Note that mobile phones can be configured to encrypt the SD card, so a corporate mobile camera phone may be suitable.

# 8 Communications and operations management

## 8.1 Unauthorised Software

Users must not make unauthorised copies of software, or download or install unauthorised software.

Further, users must not accept screen prompts to download and install anything via their Internet browser or ‘App Store’. Special care must be taken to check for where ‘tick-boxes’ on sites have been ticked by default to download software – for example to download and set Google Chrome as your default browser. Security restrictions in place on devices will prevent installation of most software by users themselves. For example, Windows 10 will deploy application whitelists to secure the system from malware and unauthorised apps.

Software, ICT systems and hardware must not be purchased without the approval of the Business Manager or Service Director. Such software may not be secure or aligned with architectural principles or it (or a suitable alternative) may also be already available at no further cost to Adoption West. Similarly, technology services (whether local or hosted, ad hoc or contracted for open-ended or defined periods of time) must not be entered into without Business Manager or Service Director approval.

## 8.2 ICT Security and Acceptable Use Monitoring

ICT can use software which runs 24 hours per day to automatically check or access all devices on Adoption West’s network. The system is used to detect unauthorised software, communications and activity as well as deploy approved software remotely.

**The software is not used to look into data files or e-mails.**

Acceptable use and links to HR documents is discussed at the beginning of this policy document.HR

## 8.3 Backups

**If you save data to your device and not to a network location, it will not be backed up. As such it will be vulnerable to loss. Your Team and Adoption West in general, may suffer if you lose data stored locally on a device, always ensure you save data to a network location (see also 8.5). If you have a work smart phone then your contacts are synchronised back to the Microsoft Exchange server automatically.**

## 8.4 Archiving information

Any data that needs to be archived should be stored on a network drive. Be aware that if you are writing/burning data to DVDs/CDs, as a media they can degenerate over time making the information they contain unreadable. They along with USB sticks/flash memory are not appropriate as a long-term storage solution for important data and must be encrypted and password protected where appropriate. Please contact the ICT Helpdesk for advice on more suitable options

## 8.5 The Internet and Cloud Services

Information and guidance is available to help with ways of securely sharing and collaborating. See the section on new technologies and new ways of working where *business grade* versions of Onedrive and other Cloud services can be used.

**Access to corporate Onedrive or network drives can be obtained by using locally available WiFi or tethering to a smartphone over 3/4G. Captive portals are another option (where you log on to a web page to access the Internet) but use of these requires a ticket with the Helpdesk and authorisation. Users need to read the security guidance supplied by the helpdesk upon approval when using this mode of access.**

**Do not** visit internet sites that might contain obscene, hateful or other objectionable material. All employee internet use is recorded in the event that ICT have to carry out an investigation, for example, checking who visited websites which introduced a virus.

**Do not** carry out any financial transactions **using your Adoption West email address**, this includes but is not limited to, online banking (Lloyds, Barclays etc.) and shopping (eBay, Tesco, Argos etc.). Websites such as these are significant targets for e-crime to harvest financial information, passwords and email addresses for identity theft.

**Do not** post inappropriate or offensive remarks, proposals or materials on the internet (e.g.

in online forums or on social media such as Facebook or twitter). Take care with information that you share to ensure that it does not compromise the reputation of Adoption West or inadvertently convey something confidential or sensitive. Also refer to Adoption West’s **social media policy** at [www.adoptionwest.co.uk](https://adoptionwest.co.uk/policies-and-procedures/)

**Do not** use the internet and personal **cloud services** to store or transfer protected data without undertaking an information governance risk assessment. Use of consumer services such as DropBox, Google Drive, Basecamp and OneDrive is not permitted under normal circumstances.

## 8.6 Email

**Never use personal email accounts (such as Gmail, Yahoo Mail or Hotmail) to transfer Adoption West data or carry out work business**. Be aware that emails are not secure (unless you are using specific secure systems such as GCSX (Government Connect) or Secure Mail (CRES) and that email delivery cannot be guaranteed. They might be intercepted or mis-delivered if you make an error in an email address. Always double-check the email address as people can have the same names or the box may have been autofilled in some email systems. Always double-check the email and attachment contents to ensure the information is appropriate for the intended recipients.

Do not send defamatory emails, or use email for harassment or to share protected information with people outside Adoption West, for example about employees, workers, suppliers, partners or customers of Adoption West. Be aware that all communications that you send or receive are recorded and can be monitored.

Never register your work email address or use your work login details (username and password) with any website to conduct personal business such as newsgroups, social media websites, online forums, internet banking or shopping websites such as Tesco or Amazon. This presents a “phishing” risk to Adoption West, see section 9.7 below. Note: Phishing is the fraudulent practice of sending emails that appear to be from reputable companies or contacts to lure the receiver into revealing personal information such as passwords, or clicking on malicious links that may contain viruses or ransomware.

Although email is the usual method, phishing can also occur by phone. For example, the caller may claim to be from Microsoft Support and requires access to your computer to assist a software problem, virus etc. Their motives can include gaining remote access to the computer to steal information or install a virus, steal banking details or obtain information to facilitate identity theft.

The calling number may often be from abroad, but some callers use techniques to spoof local numbers so the call can appear to from a local region. Always be wary of unexpected calls that attempt to obtain information.

## 8.7 Computer viruses

All users must be aware of the risk of computer viruses especially ransomware, and the serious damage they can inflict. Although we use anti-virus software extensively, new ones are constantly emerging so there is no room for complacency.

Most modern malware is inadvertently downloaded from the internet or through email. Do not pass on virus warnings to other people. Many are hoaxes designed to cause disruption in precisely this way.

Do not act on warnings that suggest you delete files from your device. They usually suggest that you delete files essential to the working of your computer.

Attachments and links in e-mails are a common and easy way to spread computer viruses: -

* **Do not** open e-mail attachments from people you don’t know
* **Do not** open unexpected e-mail attachments from people you do know, verify first
* **Do not** open any attachment from a source that looks in any way suspicious
* **Do not** forward any e-mail unless you are 100% sure of their contents
* **Do not** click on a link and enter any personal information or your password
* **Do not** use work equipment to browse internet sites you do not trust.

**DO** connect your work device to the network at least once per month for the latest patches and anti-virus updates (devices will be disabled after 60 days if not connected).

**DO** report anything you suspect to be a virus to the Service Desk and Business Manager immediately on 01454 863838 / servicedesk@integra.co.uk – especially if you have accidentally clicked on a suspect link or opened a questionable email attachment

**TIP:** Hover over a link with the mouse pointer to see if the link matches the true destination. See example below, notice how “www.mybank.co.uk” is really linking to “www.badguyhere123.com”.



Where computer viruses are concerned, *it is advisable that you maintain best practice at home with your own personal computing equipment* ***and*** *keep them up to date with the latest patches and anti-virus updates.*

## 8.8 Phishing emails

As mentioned above, phishing emails are emails that look as if they are from a legitimate organisation and usually request information. The email will ask the recipient to supply confidential details, such as your user name and password often via a website. Users must be very careful when following links in emails.

**IT staff will never ask you for your password. You should never provide your work passwords to anybody else, either over the phone, on a website or in an email as you would be accountable for all actions taken with it. Cybercriminals will go to great lengths to craft e-mails (or possibly call you) that are convincing by using detailed information they have acquired and psychology (scare tactics etc.) to obtain your passwords or other security related information.**

# 9 Access Control

## 9.1 User access management

New users will be set up on the network only on receipt of an ‘IT new starter request form’. This form needs to be completed by the line manager and authorised. This must be sent to the ICT service desk electronically. No new user will be registered without this form.

Once staff are approved to access Adoption West systems this is only within the scope of their role. Staff should not access systems unless they have explicit permission to do so, if discovered this will trigger a security incident which may lead to a disciplinary process. Furthermore, staff should not access personal or sensitive information unless they have been given permission and have a legitimate legal right to do so. Accessing data without proper cause is a criminal offence.

When staff leave, ICT use a leavers report to identify these and close all user network access.

When agency and contract staff leave, line managers are required to inform the ICT service desk. In addition, accounts for agency and contract staff are set up to automatically expire after 3 months unless line managers inform ICT that the individual continues to be employed by Adoption West.

## 9.2 Screensavers

By default, all devices have been configured with a time activated screen saver, which requires entry of your password to regain access. On smartphones this requires entry of your PIN. However, the automated screen saver is a failsafe and before leaving your workstation you should always ensure you have locked the screen to prevent others from viewing the data on your screen or gaining inappropriate access to systems and data. To lock your screen press the Control, Alt and Delete key together and select Lock This Computer.

Alternatively press the Windows Key and the letter L together.

## 9.3 Modems and other network connectivity

Modems pose a specific security threat and must not be used or installed without written permission from the Business Manager.

Similarly, personal mobile hotspots must not be used whilst connected to the corporate network.

Under no circumstances should a personal WiFi/wireless router or other device be plugged into the corporate network.

ICT staff will disconnect and remove any unauthorised modems/devices without prior notification.

Laptop computers may be supplied with a built-in modem. This should not be used without written permission by the Business Manager.

## 9.4 Passwords

Passwords are the front line of computer security and require particular attention and you should ensure that you keep it secret!

**As mentioned earlier, you are responsible for actions undertaken with your password.**

Be aware that someone might do things with your password that you would not dream of doing, would not know how to do, or that you do not even know exist.

**Do not disclose you password to anyone. Literally no-one.**

Do not allow other members of staff or ICT suppliers/contractors to know your password, or allow them to use it even if they are helping you. ICT staff may ask you for your ID, but will never ask for your password.

**Managers do not have a right to ask you for your password.**

If you need to share information, this can be done in a proper and controlled way. Call the ICT Service Desk and explain what you want to achieve. We will work to help you achieve it.

Most password checkers are only a guide, they will accept bad passwords such as “JohnSmith123” because they only check construction *not* content.

Some guidelines for passwords are: -

* **Do not**  use the same passwords for work and home
* **Do not** use the same password on different systems e.g. Facebook and Bank
* **Do not** choose ‘easy to guess’ passwords
* **Do not** write your password down unless you can hold it securely (treat any written down passwords as you would cash or credit card).
* **Do not** include your password in any automated process, such as a macro or user defined function key

Avoid passwords based on:

* months of the year; days of the week, or dates such as birthdays
* sequential number rangers such as 123, 456
* family (Edward or Richardson) or pet names (Fido or Scruffy)
* car registration numbers, postcodes or telephone numbers or company names
* Be careful about details revealed in social media such as Facebook – do not use that information in passwords or other security tests (e.g. security questions like “Who was your favourite teacher at school?”)

Passwords are difficult to deal with because they are hard to remember and we need so many of them; yet it is crucial that they are kept secret. People attempt to cope with this overload by re-using passwords or using simple password rules like adding the website to the password e.g. amazonmypassword23, facebookmypassword23. The hackers know these tricks and will exploit them!

To help keep passwords secure but also cope more easily with them, the following are examples of secure methods:

* Use a password manager e.g. Intel Truekey (this is just one example of many)
* Use passphrases e.g. 5 *random* words such as treespothighleverwaft (many systems insist on numbers or uppercase, so Treespothighleverwaft1 could be used instead – do not use this example in an actual password!)

**If you think your password may have been compromised in any way, contact the ICT service desk immediately.**

## 9.5 Remote control software

ICT staff will never remotely take over a PC which someone is logged onto without the express permission of that person. Microsoft Skype (previously called Lync) and System Centre Remote Control is the only software approved for use by all staff that has this capability.

Sometimes suppliers need to be able to provide remote support. You should not allow access to your PC without prior approval from ICT. Suppliers requiring such access will need to complete the necessary request for remote access process.

## 9.6 Connection to Adoption West’s data network

Staff must not interfere with or connect any unauthorised device to Adoption West’s data network or systems. This includes connecting hardware to a physical network connection or WiFi network.

Authorised devices are those purchased via the ICT provider. Authorised devices must be connected to Adoption West network at least once per month so that the device remains in a ‘known’ state and can receive the appropriate software, security and anti-virus updates (remember, devices will be disabled after 60 days if this is not done).

Adoption West work must not be performed on personal (non-work issued) devices except where written permission has been given by the Business Manager or Service Director.

All other devices are unauthorised, except where written permission has been given by the Business Manager. ICT staff will immediately disconnect or disable any device that is suspected to be unauthorised.

# 10 Business continuity management

In the event of a business continuity or disaster recovery event, the ICT Security Policy remains in force. Should any part of this policy require suspending it will be authorised by the Business Manager in coordination with the ICT provider and Data Protection Officer.

# 11 Compliance

## 11.1 Computer Misuse Act

The Computer Misuse Act 1990 introduced three criminal offences: unauthorised access; unauthorised access with intent to commit a serious criminal offence; and unauthorised modification of computer material.

Any member of staff identifying or suspecting such activity must report it immediately (see section 7.2 above).

## 11.2 The Data Protection Act

All use of ICT systems covered by this policy is also assumed to be covered by the Data

Protection Act.

## 11.2 Caldicott Guardian

The Caldicott review of personally identifiable information in 1977 recommended that ‘Guardians’ of personal information be created to safeguard and govern the uses made of confidential information within NHS organisations. In 2002 the Caldicott standard was extended to councils with a social services responsibility, in order to provide the basis of joint working with health.

Caldicott incorporates security responsibilities within its requirements, and is therefore linked with this policy.

## 11.3 Intellectual Property Rights

Staff must be aware of intellectual property rights, such as copyright, design rights and trademarks. Infringement can lead to legal action that may involve criminal proceedings. This warning is particularly pertinent to the use of material available on the internet as the same legal requirements apply. If you do not understand these implications, ask your line manager.

## 11.4 Software copyright

ICT are responsible for maintaining copies of all software and licences and therefore purchasing all new software. Staff should never purchase software or ICT services (including hosted ones) themselves irrespective of their value.

Refer to the Business Manager for more details about the process for purchasing software.

## 11.5 Unauthorised use of equipment

Adoption West’s ICT equipment may not be used for unauthorised purposes. This could lead to criminal or fraudulent acts, waste valuable resources, or result in damage to hardware, software or data.

**This includes inappropriate streaming or downloading of media (e.g. music and video). All internet activity is logged and can be attributable to the user logged in.**

## 11.6 System Audits

ICT gives notice that it will undertake electronic system audits (using Microsoft System Centre) to identify unauthorised, illegal or unlicensed software. These may not be obvious to users. Any such software is liable to immediate deletion without warning.

## 11.7 Compliance testing

ICT will undertake unannounced tests to assess compliance with the ICT security policies. This may involve inspection of equipment, simulated attempts to gain unauthorised access, and other similar means. Internal and external auditors may also undertake specific work to identify compliance by users.

# 12 Miscellaneous

## 12.1 Waste disposal

Storage devices such as hard disks, USB drives, CDs, DVDs and older floppy disks should always be returned to ICT for disposal. This is because they should be treated as confidential waste and be destroyed professionally in a compliant manner.

All ICT users should take care when disposing of computer printouts that may contain personal data. We encourage recycling of waste paper, but this must not compromise confidential or personal information. Confidential waste bins are provided at all office locations.

**Should you work from home or a location which is not owned or managed by Adoption West then any waste (paper, film etc.) that requires to be disposed of must be done in a compliant manner; if it contains personal or sensitive information it must be brought to a managed property and disposed of in a compliant manner,**

## 12.2 Accidental verbal disclosure of information

Staff who have access to large databases should be aware of the risks of accidental verbal disclosure of information, and take measures to prevent it.

It is important not to accidentally disclose information of a personal nature, such as the name of an occupant at an address. Caution is required against people who may approach us in order to trace or harm someone.

Staff should also be aware that accidentally disclosing information about the status of a person or an address can also compromise their security, and constitutes a breach of this policy.

**You should refer to** http://intranet/ig **for further information about the Data Protection Act and general Information Governance best practice.**

# Annex A - Staff Quick Security Guide

**DO** report unknown people entering Adoption West / council premises when they do not have a pass.

**DO** connect your device to the network monthly for the latest software updates.

**DO** take care with information that you share to ensure that it does not compromise the reputation of Adoption West or partner organisations, or inadvertently convey something confidential or sensitive.

**DO** report anything you suspect to be a virus to the ICT Service Provider immediately

**DO** use [the Bcc address field](file:///%5C%5CAWP.Internal%5CAWP%5CShares%5CAll_Shared%5CAdoption%20West%5CStaffInfo%5CICT%5CHow%20to%20Guides%5CGuide%20-%20Email%20Bcc%20%26%20email%20checks.docx) when sending invites or information to multiple external recipients to ensure identities and email addresses are not disclosed to other recipients

**DO** check the email recipients before sending , especially if email addresses are completed with the autofill function

**DO** open and check attachments before sending external email to ensure it is the correct file and version that you are sharing

**DO** upload attachments from folders rather than from recent / suggested files in Outlook to ensure you are selecting the correct file

**DO** use hyperlinks rather than attachments for internal email (so that any incorrect recipients will not be able to access the linked information)

**DO** ensure when sending links to shared document folders (e.g. using Sharepoint or Onedrive) that the folder only contains information that recipients should have access to

**DO** only populate a word template once it’s copied and saved separately (template files should be saved as template versions to avoid inadvertently saving and then sharing other protected information on a document that has been re-used.

**DO** be extra vigilant when sharing a file that has been edited to remove other protected information (e.g. relating to other service users) to double check that only the information that needs to be shared is included

**DO** check there are no hidden tracked changes by selecting ‘Review’, ‘Tracking’, ‘All Markup’ and if it’s a final document then ensuring all changes are accepted and it’s clean of any marked up changes

**DO NOT** disclose your password to anyone. **Literally no-one!**

**DO NOT** leave your laptop at your workstation overnight, even in Adoption West / council premises, ensure it is locked away in a secure cupboard or drawer.

**DO NOT** open e-mails from unknown people or from people you know which appear suspicious, e.g. an unexpected subject, unusual content or no appropriate signature block.

**DO NOT** open e-mail attachments that are unexpected or that look in any way suspicious.

**DO NOT** visit internet sites that you do not trust or that may contain objectionable material.

**DO NOT** post inappropriate or offensive remarks, proposals or materials on the internet (e.g. in online forums or on social media such as facebook or twitter).

**DO NOT** use the **internet** and/or **cloud services** to store or transfer protected data without undertaking an information governance risk assessment and speaking to ICT.

**DO NOT** register your work email address for personal use, this includes social media sites such as facebook/twitter, banking (e.g. Barclays) or shopping (e.g. Amazon, Tesco).

**DO NOT** send defamatory emails, or use email for harassment or to share protected information with people outside Adoption West.

**DO NOT** pass on virus warnings to other people. Many are hoaxes are designed to cause disruption in precisely this way.

**DO NOT** click on a link in an email and enter any personal information or your password

**DO NOT** act on warnings that suggest you delete files from your device. They usually suggest that you delete files essential to the correct working of your computer.

**DO NOT** forward email conversations to new recipients without checking or deleting the email thread below

**All employee computer and internet use is recorded in the event that an investigation is required, for example, checking who visited websites or downloaded and/or installed software.**