IT Security Summary

IT security 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 risk of fraud and inappropriate access to confidential data.

Top computer security tips:

Passwords

* + The use of strong passwords is essential in order to protect security. You are responsible for action undertaken with your password, DO NOT disclose your passwords to anyone. ICT / site administrators will never ask for your password. Passwords and pins must be changed regularly, you will be prompted when it is time to change your password. If Users suspect their password may have been compromised or used by another person, they must immediately change their password (using ‘My Account’ > ‘Security & Privacy’ > ‘Change Password’) and report the incident to the Site Owner for investigation by contacting info@adoptionwest.co.uk.

Physical Device Security

* If your computer equipment is not suitably protected it is easy for criminals to steal data, infect your computer, or steal the equipment itself. Do not leave your computer unattended and unlocked; if you do you are putting data in jeopardy. If you need to leave your computer for some time, you can quickly lock your account so no one can access it.
* To do this, do one of the following things:
•Press the Windows logo key and the letter ‘L’ at the same time
•Press Ctrl+Alt+Del and then click Lock this computer
* Portable ICT equipment should be locked away out of sight overnight and if travelling with your device you should keep it with you whenever possible. Never leave it unattended in a vehicle or a public place. Never leave a device on a car seat, even if you are in the car it could be vulnerable when you are stationary e.g. at traffic lights, or whilst parking. If your device is lost or stolen follow the data breach advice below.

Data Breach advice

* An information security incident or concern is any action that may compromise the confidentiality (i.e. accuracy or completeness), or availability of information. Also referred to as a data breach.
* This includes both information stored and processed electronically, and information stored in other forms such as paper.
* Compromise of confidentiality, integrity or availability could result in reputational damage, detrimental effect on service provision, harm to individual(s), legislative non-compliance and/or financial costs.
* All employees, partners, contractors and agents have a duty to report any observed or suspected information security incidents or security concerns.
* Any information security incident or concern must be reported at the earliest possible stage to info@adoptionwest.co.uk

Email

* Email is an excellent communication tool, however, there are reports in the media most days of incidents where criminals have used email to deliver unwanted material, including viruses and malware, which are at best annoying and at worst, malicious. Such ‘malware’ could cause considerable harm to your device and could potentially lead to data breaches, where criminals steal data or even your own personal data and passwords.
* Phishing emails are a scam where criminals send emails to try and trick you into giving them personal information that could lead to fraud, data breaches, computer viruses and spyware with the potential to infect other networks.
* Never use personal email accounts to transfer organisation data
* Remember that emails are not secure unless you are using an approved secure email system e.g. GCSX or Government Connect
* All communications that you send or receive are recorded and can be monitored.
* Be cautious of any email that does not use your proper name e.g. addressing you as Sir/madam or Dear customer
* A website address that seems very similar to the proper address may be difficult to spot, but even a single character difference means a different website
* Delete any email which requests personal information such as your username, password or your bank details.
* Do not click on a link you did not expect to receive
* Do not open attachments from unknown sources
* Do not forward emails you suspect as being spam
* Do not reply to emails from unknown sources
* Delete emails to your account appearing to come from banks, eBay,
PayPal or similar institutions or any email that is asking you to supply personal information online. Email filters will block a large proportion of these types of emails but you must be vigilant. ICT Staff / site administrators will never ask for login details or passwords.

Viruses

* If your computer slows down, you are getting unexpected activity or messages on your computer or your data files become corrupt or go missing then you could have a virus. Please report anything you suspect to be a virus to info@adoptionwest.co.uk immediately.

Do:

* keep personal data safe – it’s everyone’s responsibility
* think before you speak – a disclosure can be spoken as well as written
* ensure you are authorised to print information or to take hard copy/paper files off site
* wherever possible use remote access (or SharePoint) instead of taking hard copy information off site
* use confidential waste bins / sacks in the office for personal, financial and sensitive information, shred before you dispose if away from the office
* ensure personal data is accurate and up to date
* be aware of retention and disposal guidelines – data cannot be kept indefinitely
* know who you are allowed to share information with (data sharing protocols)
* when you do share information always double check that the recipient is the correct recipient
* be aware of data protection and information governance [policies and procedures](http://intranet/content/CEandCR/Sections/IG/policies.htm)
* ask for advice if you’re not sure

**Don’t:**

* ignore potential risks – report incidents or concerns to info@adoptionwest.co.uk
* email sensitive information unless you are sure it is encrypted
* store password information with your laptop / device
* leave your laptop / device unattended
* leave your laptop / device in your car. If this is unavoidable, temporarily lock it out of sight in the boot
* store or send personal data on removable media (USB pen drives, CDs etc.)
* never store sensitive information on an unencrypted mobile phone or tablet
* assume you can disclose personal data to another member of staff
* leave faxes and print outs lying around – even accidental disclosures are a breach
* use personal data for a different purpose without considering data protection
* write any comment about any individual that is unfair or untrue which you would be unable to defend if challenged. You should assume that anything you write about a person will be seen by that person.