Information Security

STAFF GUIDANCE

Contents

1. Antivirus Software

- Run antivirus software of your choice on your devices
- Perform a full scan from time to time and follow-up results

The College us the Microsoft Windows Defender antivirus software on all its devices (including equipment on loan to staff).

On your home computer if you are running Windows 8 or above, you can run the free Windows Defender antivirus software which comes with your machine to prevent you falling prey to easily preventable infections. This software should run in the background without impacting the performance of your system.

Periodically – every month would be a good pattern – it is worth running a full scan of your system to see if anything else has been picked up. You may wish to use an alternative program to do Microsoft Defender, such as from Symantec, Sophos or McAfee, as they could pick up problems your Microsoft Defender software missed. However, it is not advised to have two antivirus programs running background scans as they can interfere with each other.

If you have any problems enabling Microsoft Defender on your home computer or If your computer has been affected by a problem that this software detects, please report it to the Computer Support Team on ext 4134.

You should also consider scanning or reporting your machine if it starts to display unexpected behaviour, such as periodically running slowly or overheating, as these could be signs of unwanted software running in the background.

2. Backups

- Ensure your data is backed up and contact the IT Help Desk if you need support with this.
- Backups protect you against information loss
- A backup is only safe if you know you can restore your data from it

Backups provide a strong defence against information loss. Data recovery may be impossible or prohibitively expensive from a broken device but having recent copies of your information allows you to get back to work quickly.

The best location to store your files is on the College network. On the network, automatic backup happens nightly. If the data is sensitive, the backup version should also be protected.

3. Cloud Services

- Don't use non-College cloud services for College data without discussing it the Data Protection Officer first.
- Convenience has to be balanced against security concerns. Always consider College-based alternatives first.

Cloud services – including well-known services like Dropbox or Google Drive are convenient but not always suitable because they put copies of your data in places you have no control over for example outside the European Union. Additionally, services often require agreeing to the provider's terms and conditions and you can't enter into a contract on behalf of the College. You cannot guarantee on deletion, the information is removed from all servers it was stored on.

In many cases, there are College provided services that will provide an equivalent or better solution. For example, you can use the College's Virtual Private Network (VPN) or Virtual Desktop Infrastructure (VDI) to access your network drives from home. This also avoids keeping a copy of files on non-College machines.

4. Email

- Contact Computer Support if you encounter a virus or phishing messages that appear to come from the College network.
- Email is widely used but is insecure without taking uncommon precautions
- You can't unsend an email so consider before you commit to it
- Be cautious about the content of emails you receive

When sending emails, you should be careful about the written record you are creating. When including people in an ongoing email conversation, it may be sensible to remove older messages to keep the discussion appropriate to the new scope. You should also consider how aware the recipients are of each other; often it is useful to understand who else is in the group but if, you do not have permission to distribute email addresses of group participant to external contact use the Blind Carbon Copy (BCC) option. Remember that once the email has been sent, it has gone outside your control and could end up forwarded and stored on systems you would not consider trustworthy.

When you receive emails, you will get a certain amount of spam – unsolicited marketing material and other junk. The College spam filters reduce the amount you see but, to avoid important messages getting lost, are set not to be too zealous. If you see an email that tries to impel or entice you to click on a link, be very cautious. This may be what is known as '**phishing'** and this class of spam has become quite hard to spot. Watch for signs like a sense of urgency or a link that is complex or shows a different address when you hover over

it. Note that you cannot rely on the apparent sender of the message as this information is easily forged. Please advise the Computer Support of phishing messages that pretend to come from Accrington and Rossendale College; other phishing attempts can be deleted.

You should also be cautious of attached files. If unexpected, treat with caution even if they appear to come from a trusted source. If you realise you have been caught out, contact the Computer Support Team on ext. 4134 to arrange immediate assistance.

Do not keep sensitive personal information, such as learner personal data on your local hard disc or in your email any longer than necessary. Where possible, find other ways of sharing and using such information.

5. Encryption

- Mobile devices containing personal data, including USB stick and laptops, must be encrypted. Please see Data Encryption Guide

Data Encryption Guide.docx

- Encryption offers very strong data protection
- Depending on your work, there may be situations where it is a definite requirement.

Encryption jumbles data so that it can only be unlocked by providing a key, often in the form of a password. There are many ways things can be encrypted but, if you use a reputable method, the main risks to your data are either that someone steals your key or that you forget it!

Encryption can be applied at various levels. For example, you can protect an individual file. Microsoft Office products since Office 2007 provide very strong encryption protection. Please refer to the Data Encryption Guide for more information.

Encryption can also be applied to external drives; you can obtain a USB stick with hardware-based encryption from the College library shop.

When you use websites with URLs beginning HTTPS, indicated in most browsers with a padlock icon, information is automatically encrypted between you and the server at the other end. This is important when sending or receiving secure information, including logging in to a system with your username and password.

6. Location and Being Overlooked

- Be aware of your surroundings
- Not all networks are trustworthy
- Avoid your screen being overlooked by unauthorised people

Mobile devices and cloud services give you freedom to access information in many places other than your staffroom or office but this creates additional risks.

When accessing websites and data, you are sending and receiving messages across network connections. Where possible, it is sensible to use secure websites, which will have addresses starting https:// rather than http:// as these automatically encrypt your communication with the site.

From networks you cannot confidently trust, such as hotel and airport Wi-Fi hotspots or at home, use the College's Virtual Private Network (VPN) or Virtual Desktop Infrastructure (VDI) software to provide a secure tunnel into the College network.

In public places, you should be appropriately cautious about what devices you are seen to be using to avoid becoming a target for thieves. This applies to the risk of somebody stealing your device but also the possibility of someone reading or photographing your screen.

In any location, do consider whether your screen and keyboard are overlooked, for example through nearby windows. You may need to take preventative measures and you must lock your screen when you leave it unattended. Even in the College buildings, be careful about security and take measures such as shutting doors when you leave a room empty.

7. Mobile Devices

- If you use mobile devices, take additional precautions to protect the data from loss or damage

Mobile computing and storage devices (laptops, USB / memory sticks, smart phones, tablets, etc) are relatively high risk, because they can be easily lost or stolen. It is essential that such devices are properly secured. This includes applying the available device passcode from the operating system, using at least a 4+ character passphrase or PIN to secure access. If your device does not allow this, it should not be used for College data, including logging into email or other accounts

8. Passwords

- Passwords should be at least 10 characters long and use more than one type of character
- Longer passwords are stronger
- Change it regularly—once every six to twelve months.
- Change it if you have the slightest suspicion that the password has become known by a human or a machine.
- Avoid typing it on computers that you do not trust; for example, in an Internet café.
- Never save it for a web form on a computer that you do not control or that is used by more than one person.
- Never tell it to anyone.
- Never write it down but do find software or other systems to help manage them.

For many systems, a password is still the first line of defence. Each password should be long and reasonably complex. Use at least 10 characters and preferably 15 or more. You should also include some mix of upper and lower case letters, numbers and symbols; this ensures hackers have to use the widest possible character set to build their guesses.

You may find it helps to think in terms of shorter chunks – for example, three sets of five characters. Make sure you can type your passwords accurately, finding patterns that fall under your fingers – but avoid simple runs of characters from the keyboard, like *qwerty123456*. Using numbers and symbols to stand in for $imilar characters is of limited value because it is hard to remember which ones you chose but easy for a hacker to create a ‘dictionary’ including common substitutions.

You should use different passwords for different systems and change them periodically. The College network security policy require a half yearly change. More frequent changes do not necessarily increase your security but may be required by particular systems you connect to. You must not write your passwords down in plain text but may find it useful to investigate password management software and systems such as LastPass / Dashlane. You should also not share your password with others or allow them to access resources under your account.

9. Protecting Your Computer

- IT staff can assist with physical and software security
- Lock your screen before leaving your computer unattended
- Use physical security to stop thieves being able to get to and take away your devices
- Apply software security updates and keep antivirus software running

You must take reasonable steps to protect the computers you use. For example, lock the screen before walking away from the device even if you anticipate that you will only be gone for a minute (Windows: Windows key + L). It is recommended that you shut down your computer down at the end of the day.

Hardware:- Physical security should be considered wherever possible. Portable devices must be either be shackled in place or locked away when left unattended. Locks should be used when rooms or furniture is not in use; staffrooms and open plan offices should not be assumed to be secure. Confidential data should be kept under lock and key when not in use.

Software security should be maintained. If you can install software on your machine you should only do so from reputable sources. They should be updated with patches and you should remove programs you installed but no longer use. You should also have a modern antivirus software (Microsoft Defender by default, unless you have you have decided to use an alternative) running on your machine. See also the section about software and downloads.

10. Reporting Security Issues

The following types of security incident should be reported immediately to the Computer Support Team:

- Lost or stolen College owned devices
- Malware infections
- Suspected hacking or unauthorised access
- Unintentionally emailing sensitive information to the wrong recipient

Suspected incidents should also be reported for investigation. For example, you may suspect hacking if you see the College website with odd advertising links. You do not need to report viruses that are blocked or 'Potentially Unwanted Programs' your antivirus software picks up but may wish to discuss with the Computer Support Team to find ways to avoid more serious problems in future.

If you are not sure about whether an email contains a phishing link or malware, do check with colleagues or refer to the Computer Support Team

11. Software and Downloads

- If unsure about software and downloads, please check with IT staff
- You must make responsible use of your network connection

ICT Acceptable Use Policy.pdf

Accessing the College network or being able to install software is a privileged position. You should only install software from reputable sources and ensure that they make responsible use of the College network. Some lectures or presentations may require the use of streaming media services such as YouTube. However, the College only has finite bandwidth to share among all users so it is not appropriate, for example, to spend all day listening to Internet-based radio services.

You should also exercise discretion in files you download. Avoid, for example, illegal copies of films and music. The sources for those material are often infected with malware.

Network traffic is monitored by the College. Although care is taken not to infringe your rights, there are records that could be traced to you so remember your accountability and responsibility when making decisions about what to bring onto the College network.

12.Hard / Paper Copies

- Do not print sensitive information on printers in public spaces

Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

When sending confidential data by fax, you must ensure you use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

When sending confidential documents by post, whether internal or external post, you must ensure that the envelope is sealed securely, marked 'Private and confidential', and addressed correctly. Recorded delivery must be used for confidential documents sent by external post.

When printing to hard copy confidential documents always explicitly ensure the destination printer is correctly selected and set to pull printing. (Pull printing is a printing feature where a print job is held on a server and released by the user at any printing device by use of their id card)

13.Retention and secure Data Destruction

- Ensure that you understand the College Document retention Policy and Schedule
- Emails can be deleted by selecting delete and emptying your deleted items folder.
- Personal data printed on paper must be shredded or disposed of as ‘confidential waste’ in confidential waste bins.
- Hard drives of redundant PCs must be wiped clean before disposal or if that is not possible, destroyed physically.

Appendix 1:

Quick Reference Guide

Handling Personal Data Offsite

- Avoid processing personal data offsite whenever possible.

- Be vigilant if you are undertaking work off-campus using personal data such as individualised learner data, reference requests or examination scripts or results. Strict security measures must be applied to the transportation and storage of all such data E.g. password protection, encryption or secure managed file transfer.

- Use the College's central and secure shared I-drive to store and access personal data and sensitive information; this helps to ensure that only legitimate users have access to it.

- Use the IT-authorised remote access facilities such as Virtual Desktop Infrastructure (VDI) that are both secure and encrypted to access personal data and sensitive information on the central servers instead of transporting it on mobile devices and portable media.

- Do not use non IT-authorised third party Cloud services, like Dropbox or Google Drive when processing high risk personal data or sensitive information. The data might be held outside the EU.

- If there is no option but to use mobile devices, portable media or email for high risk personal data or sensitive information, use encrypted devices or encrypt the data.

- Do not use personal equipment, such as home PCs or personal USB sticks, to process high risk personal data or sensitive information.

- Always keep personal data and work related information separate.

- Avoid sending high risk personal data or sensitive information by email or using email to store such information. If you must use email to send this sort of information, encrypt it. If you are sending unencrypted high risk personal data or sensitive information to another College email account, indicate in the email subject line that the email contains sensitive information so that the recipient can exercise caution about where and when they open it.

- Do not process high risk personal data or sensitive information in public places. When accessing your email remotely, exercise caution to ensure that you do not download unencrypted high risk personal data or sensitive information to an insecure device.

- Electronic keys for encryption, e.g. passwords, must be appropriately managed so that the College can always access the information.

Examples of

Personal Data and Sensitive Information

- Any set of data relating to more than 50 living, identifiable individuals, including, but not limited to, students or staff.

- Any set of data relating to 10 or more living, identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary

- Information relating to 10 or more students' programmes of study, grades, progression, or personal and family lives.

- Any set of data relating to 5 or more living, identifiable individuals' health, disability, ethnicity, sex life, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence.

- Information provided to the College in confidence, e.g. data relating to safeguarding.

- Health records of any living, identifiable individual.