Central College Nottingham Information Security Policy

DRAFT 3.0

February 2016

CONTENTS AND TOPIC AREAS TO COVER

1.0 INFORMATION SECURITY POLICIES

1.1 Key principles

The objective of the College's Information Security Policy is to ensure that **all information and information systems (information assets) which are of value to the College are adequately protected against the adverse effects of failures in confidentiality, integrity, availability and compliance with legal requirements which would otherwise occur.** Achieving this objective will largely depend on all members of the College complying with this policy.

The College has adopted the following eight principles to underpin its Information Security Policy:

1. Information will be protected in line with all relevant College policies and legislation, notably those relating to data protection, human rights and freedom of information.
2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
3. Information will be made available solely to those who have a legitimate need for access.
4. All information will be classified according to an appropriate level of security.
5. The integrity of information will be maintained.
6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
7. Information will be protected against unauthorised access.
8. Compliance with the Information Security Policy will be enforced.

So how do the key principles relate to me?

The above underpinning principles of the Information Security Policy are best presented as a checklist of do's and don'ts. If you work according to these do's and don'ts then you will find that you are working within the College's Information Security Policy.

1.2 Do's and don'ts

	Do		Don't
✓	Seek advice from the IT Service Desk if you are unclear about any aspect of information security.	✗	Disclose your password to anyone. See further information on keeping your password safe.
✓	Report any loss or suspected loss of data. Find out how to report lost or stolen hardware or data.	✗	Use a personal email account for conducting College business. See further information on using College email.
✓	Change your password if you have any suspicion that it may have been compromised.	✗	Undermine or seek to undermine the security of computer systems.
✓	Ensure that personally owned equipment which has been used to store or process College data is disposed of securely. See further information on hardware and data disposal.	✗	Make copies of restricted College information without permission.
✓	Encrypt your mobile devices and make sure that restricted information is always encrypted before it's sent to others. See further information on encryption.	✗	Provide access to College information or systems to those who are not entitled to access
✓	Password protect your personally owned devices. See further information on mobile security	✗	Use your College password as the password for any other service. See further information on keeping your password safe.
✓	Keep all of the software on your personally owned devices up to date. See further information on protecting your computer.	✗	Connect personally owned storage or mobile devices to College owned equipment if you are a member of staff or student.
✓	Comply with the law and College policies.	✗	Send unauthorised bulk email (spam).
✓	Be mindful of the risks of using open (unsecured) Wi-Fi hotspots or computers in internet cafes, public libraries etc. See further information on working offsite.	✗	Leave your computers unlocked when left unattended.
✓	Do assume that Information Security is relevant to you. See the Information security policy for comprehensive information on all aspects of information security at the College.	✗	Leave hard copies of confidential unattended or unsecured.

1.3 Information Security Policy Documents

- View the Information Security Policy documents
- View the key underpinning principles of the Information Security Policy
- View a checklist of do's and don'ts

Information is a vitally important College asset and we all have a responsibility to make sure that this information is kept safe and used appropriately. Without due care, personal, research or business information can be misplaced or leaked, which is a big enough problem in itself without the added difficulty of having to protect it against increasingly proactive and sophisticated attempts at theft.

Therefore, the College has adopted an Information Security Policy that complies with stringent legal requirements and provides the necessary assurance that data held and processed by the College is treated with the highest appropriate standards to keep it safe. The aims are: to raise your awareness to avoid inadvertently causing others inconvenience through disclosure of data; to avoid breaking the law; to avoid causing the College financial and reputational damage.

The majority of organisations know the dangers of information security breaches and some have suffered intellectual theft, serious reputational damage and in some cases fines for negligent management of data. We all have a requirement to work within the guidelines of the policy and by doing this you can help ensure the safety of your own data and that of others.

In simple terms, the most common causes of data loss or leakage can be avoided by:

- Making sure that only those who need access to data have that access.
- Not storing information where it can be accidentally exposed or lost, e.g. unencrypted USB drives and laptops.
- Making sure that if data has to be transported it is done so securely using encrypted devices or channels.

1.4 Top ten tips

1. Know what constitutes restricted data
2. Process restricted data on secure CENTRAL computers only and do not store restricted data on non-CENTRAL equipment
3. Encrypt restricted data to transport or convey it and fully disk encrypt your laptop/ netbook
4. Share restricted data only with those with the right and need to view it
5. Do not make copies of restricted data
6. Lock away unsecured restricted data and lock your door if leaving your room unattended
7. Never share or disclose your CENTRAL password or use it for non-CENTRAL services

8. For CENTRAL business use your CENTRAL email account and a CENTRAL-recommended secure email client
9. Securely erase data before disposing of hardware and storage
10. If in doubt about data, ask advice from the Data Protection Officer.

2.0 COLLEGE DATA AND YOU

2.1 CENTRAL data classifications

What constitutes restricted data at CENTRAL?

'Restricted' data relates to all data that is not categorised as 'public' or available to the public that could, by any means identify a living individual. As a data Controller we must establish the types of data we process and the risk these represent should this data be lost, destroyed or corrupted either accidentally or maliciously.

There are many different types of data processed at the College and will have many levels of restrictions and access controls which mitigate the 'risk'. The matrix below identifies some of these and classifies their owners and their uses. This is not an exhaustive list.

OWNER/S	DATA TYPE / ACCESS	LOW	MEDIUM	HIGH
Human Resources / Finance/ Senior Management	Restricted access controls / restricted to limited number of authenticated users			May include Sensitive personal data relating to: Pensions / salaries / health records / sickness / bank accounts / disciplinary / Contracts / Funding
Registry / Admissions / MIS / Safeguarding team / Frontline / HE Team / Student Finance / Curriculum	Restricted access controls / restricted to limited number of authenticated users			May include sensitive personal data Inc.: Name, Address, NI no, Disability, Criminal Convictions, Household incomes / Ethnic origin
Exams	Restricted access controls / restricted to limited number of authenticated users		Certificates would represent a risk of loss from fraudulent use or loss where held with other identifiable data	May include sensitive data relating to subjects personal details and examination results / access to awarding bodies systems
Timetables	Restricted access controls / restricted to limited number of authenticated users / primarily to prevent funding issues		May relate to a subjects personal timetable and identify movements	
Estates / H&S	Restricted access controls / restricted to limited number of authenticated users – However majority of data will be public	Risk Assessments as do not identify subjects only practices	Health and Safety Documentation – Where in an emergency situation the rules do not apply however any documentation must still be protected	CCTV footage / imagery may contain identifiable credible footage of subjects / Archived documents
Students	No access controls required only log in and password	Will relate only to student – generally course related		Risk could be escalated where data loss would cause harm or distress
Public / Marketing Team	N/A – However Marketing Team will own what is published in line with Sector and legislative requirements	Data relating to public funding / College Activities / Courses / course fees /Publication Scheme / Service standards		Risk could be increased where data held is used for direct marketing purposes

No restricted data, of any kind, should be stored anywhere offsite other than on approved College systems.

2.2 Your CENTRAL password

The good practice guidelines below should be common sense, but it is startling how often these rules are breached by otherwise sensible and computer-literate staff and students.

Good practice guidelines for keeping your CENTRAL (or any) password secure:

- Don't let anyone know your password (this includes emails and phone calls purporting to be from the CENTRAL IT Support Helpdesk of from IT Support Helpdesk Staff - remember, CENTRAL IT Support Helpdesk Staff will never ask you for your password).
- Change your CENTRAL password if you think that it has become known to others.
- Do not use your CENTRAL password for any non-CENTRAL accounts.
- Don't share a password amongst a group of people, even if this seems an easier solution than asking for new accounts to be set up - always ask for new accounts or shared folders to be set up rather than sharing passwords.
- Don't share your password with casual staff or ask another member of staff to share their password with casual staff - ask for a new account to be set up for each new casual staff member that you employ.
- You must not use an identifier (email address / username) allocated to someone else or allow anyone else to use your username or email address. You must never share your password with anyone - not even the IT Support Helpdesk.
- If you cannot log in for any reason, we recommend you check your password and then contact the IT Support Helpdesk and give them the message the form gives you.
- Always use strong passwords.

Good password choices are:

- A truly random sequence of mixed case letters, digits and punctuation marks. However if you have to write it down in order to remember it, it is not a good choice.
- A mixed-case phrase with one or more punctuation marks inserted somewhere in it.
- A sequence composed of the first letters of each word of a phrase. Book titles and authors can often be used in this way. For example 'The Boy in the Striped Pyjamas'

by John Boyne could give a password of TBitSP#byJB. Avoid common phrases and very well-known works when using this method.

Issue of Passwords

- Students set their own password when registering on line for the first time
- Staff can obtain their username from their department and use the self-service system for password issue or they can visit the IT Service Desk to obtain their account details.
- Departments will provide information regarding servers or systems they manage where they do not use your CENTRAL credentials
- Must not be one of the last three passwords you used for this account.

How can I avoid having to share passwords?

- Instructions on how to set up a delegated account (shared mailbox as was) can be obtained from the IT Support Helpdesk:
- Phone: 0115 884 2299.
- Online: http://helpdesk.Centralnottingham.ac.uk
- The IT Support Helpdesk can issue short-term (which expire within 24 hours) CENTRAL visitor accounts for bona fide visitors to the College. In some areas this responsibility is delegated to departmental administrators or IT staff.

Changing Passwords

- Password changes are currently enforced after 42 days.
- You can change your passwords via the web form.
- You can use this form as long as you know your CENTRAL password and can change that.
- If you forget your CENTRAL password, you may be able to reset it yourself on line by using the reset page. If this is not successful, please contact the IT Support Helpdesk.
- If you believe you have been locked out, please contact the IT Support Helpdesk.

Usernames

- The user name (issued by the IT department) is in the format ‘john.smith’ made up of the first and surname, separated by a full stop.

2.3 Email and CENTRAL data

Confidential College data and email do not mix well. Keep the following recommendations in mind when dealing with College data.

Can I send restricted or sensitive data by email?

Restricted CENTRAL data and data classified as "sensitive" under the Data Protection Act must not be sent by email unless encrypted. Emails might be intercepted or mis-delivered en route - sending restricted data in an email is much the same as sending it on a postcard: you don't know that anyone will read it, but you should know that it is a possibility. Sending this sort of data by email could be considered a breach of confidentiality and if personal data is lost or disclosed, the College could suffer a heavy fine as well as suffering damage to its reputation.

For recommendations on email encryption and on preferred alternatives for conveying restricted or personal data see the following sections:

- Email encryption
- Windows Encrypting File System (EFS)
- Encrypting mobile and storage devices

What else do I need to know about good practice with emails?

- Do *not* use a personal email account to conduct College business. Using a personal email account for CENTRAL business can mean a lack of audit trail and could also result in inadvertent breaches of the Data Protection Act.
- Consider your message recipients' reasonable expectations of privacy with respect to their email addresses and do not divulge them unnecessarily. Do not, for example, always include all recipient addresses in the "To:" or "Cc:" message headers when sending an email. Consider using the "Bcc:" header instead. Depending on the message content, divulging one person's email address to others may constitute a breach of the Data Protection Act.
- Many email applications store emails to local drives, which can be a security risk if computers or mobile devices are lost, stolen or disposed of non-securely, so use a College recommended email client to minimise the risk of this happening.
- If you need to use something which stores emails for mobile working, it should only store a few emails from the inbox and not your entire archive. Delete any locally stored emails when you are finished with them.

Limited use of your CENTRAL email account for personal business is acceptable - though you should be aware that in certain circumstances your email account may be accessed by the College. Instead you might want to set up one or more personal email account with Hotmail, Google or similar. Bear in mind though that these may not be 100% secure.

Why and how to use BCC when sending emails

BCC: (Blind Carbon Copy) is an email field to which you can add several recipients, while the addresses remain hidden from everyone, unlike the addresses placed in the To: or CC: (Carbon Copy) fields, which are visible to anyone who reads the message.

Why should I use the BCC field?

While sometimes putting all the addresses in the To: or CC: fields is appropriate and in some situations may even be required, most of the time it is unnecessary and harmful. As a base rule for determining whether we should use the BCC: or either to To: or CC: fields, we should answer this question: does each recipient of this message need to know who every other recipient is, as well as their email addresses? The cases in which the answer is "yes" will probably be when dealing with work-related emails or emails exchanged between a group of friends **that already know each other**. And even in those cases we can make the recipients known by listing their names at the beginning or end of the email, and still respecting their privacy.

In all other cases we should always hide the recipients' email addresses in the BCC field.

The majority, if not all email programs, allow you to add recipients to the BCC field. Some of them may hide the field by default but there's always a button or configuration option to make it visible.

Note that some email services or programs may require that you put at least one email address in the To: field, like Yahoo! Mail, for example. In these cases you can use your own email address, since that will always be visible to everyone because you're the one sending the message.

Email threats

Although the majority of malware is introduced through browsing of unsafe sites, email is still a major source of concern with regard to spreading of malware and of phishing for personal details. Be sensible when reading your email and follow these basic guidelines:

- Install anti-virus software, firewall software and anti-spyware software and keep it up-to-date by installing updates regularly.
- Don't open file attachments if you don't know the person the message is from - just delete it.
- Don't click on links in the message body if you don't know who the message is from - just delete it
- If someone you know sends an unexpected attachment or asks you to click on a link, contact them to check that they sent the message - if they didn't, delete it and suggest they check their computer for malware
- Filter out unwanted spam - some spam will always get through, but most won't
- Do not transmit sensitive or confidential information - emails and instant messages can be intercepted and read
- If your instant messaging client asks you to fill out a profile of yourself, do not give unnecessary personal information

- Download security patches for your instant messenger and upgrade when available - new upgrades fix security holes
- Apart from the threat of infecting your computer with malware, emails and instant messages are commonly used to *phish* for personal information. Any personal information you give away could help someone to steal your identity.

2.4 Encryption advice

Encryption is a means of preventing anyone other than those who have a key from accessing data, be it in an email, on a computer or on a storage device. In all cases you need to consider the security of the encryption key(s) and it is recommend that you lodge these securely with a trusted third party (who, preferably doesn't have access to the files) so as to ensure their availability in the event of key loss.

The Information Commissioner has made it clear that personal data subject to the Data Protection Act must be encrypted whenever it is "transported" or "conveyed". This includes data stored on physical media (laptops, CD/DVDs, USB drives, etc.) as well as data transmitted electronically (College email, Google Drive, etc.). Failure to do so is a breach of the 7th data protection principle and could result in action being taken against the College in the event of data loss. Encryption of data using CENTRAL-approved software and/or devices is one method of protecting against breaching the above data protection principle and should further be used if transporting or conveying restricted CENTRAL data.

2.4.1 Email encryption

Our current email filtering system does not support encrypted email therefore you must not, under any circumstances, use email to send strictly confidential College data (including data that is classed as 'sensitive' under the Data Protection Act). This includes data in both the email and any attachments. Do not, under any circumstances, use Hotmail or other external email service for sending or storing restricted College or sensitive data.

Rather than use email, if possible, encrypt files and store them on a Central file server and ensure that only those who should have access do have access.

2.4.2 Windows Encrypting File System (EFS)

Encrypting File System (**EFS**) is a feature of Windows 7 (and later) that you should use to store information on your hard disk in an encrypted format. Encryption is the strongest protection that Windows provides to help you keep your information secure.

2.4.3 Encrypting mobile and storage devices

Encrypted mobile devices (laptops and netbooks in particular) should always be powered down and not simply put into 'sleep' mode when they are at risk of loss or theft (e.g. when

they are in transit). If in sleep mode then encryption is circumvented and the data can be accessed.

All members of the College must act in accordance with the relevant laws and College Information Security Policies.

If you transport restricted College data, or data that is classed as "sensitive" under the Data Protection Act, on any mobile or storage device, be that a laptop, notebook, USB stick, or CD/DVD or similar, then that device must be encrypted. It is further recommended that any mobile or storage device containing restricted data that is only used within the College is also encrypted and/or locked away when the office is left empty in case of theft.

If you decide to encrypt your personal computer, be aware that there are pitfalls - the most common problem is losing access to your data. Also remember that you must not process or store restricted College data on any non-CENTRAL computer.

For guidance on how to encrypt mobile and storage devices, please consult the IT Support Helpdesk.

2.4.4 CENTRAL-approved USB drives

CENTRAL staff should only use CENTRAL approved encrypted USB drives and under no circumstances should any other device be used.

For guidance on how to acquire the approved USB drives then please consult the IT Support Helpdesk.

2.5 Working offsite

If you are processing College data from outside of the College's networks then work according to these do's and don'ts and you will find that you are working within the College's Information Security Policy.

	Don't		**Do**
✗	Don't process restricted CENTRAL data on a non-CENTRAL computer.	✓	Do request to use a CENTRAL-owned laptop or other hardware if necessary.
✗	Don't set your browser to save passwords for you (especially CENTRAL passwords).	✓	Do use private browsing mode and/or regularly erase your browsers history - especially if you're using a public computer.
✗	Don't needlessly transport CENTRAL data	✓	Do use the College's virtual private

	from one site to another - and never transport restricted or personal data unless it's encrypted. View encryption advice.		network (VPN) or a terminal server client to access data. This system provides you with a full desktop, which works in exactly the same way as if you were sat at a PC on Campus. Do use CENTRAL-approved encrypted devices.
✗	Don't copy data in bulk when you only need a bit of it.	✓	Do only copy the data that you need to do the job in hand.
✗	Don't use public computers to access any College services that require you to log on: public PCs in hotels, airports, Internet cafes and libraries are almost always infected with malware.	✓	Do be cautious about using anyone else's computer to access College services that require you to log in.

2.6 Mobile and removable devices

Make sure that you know the reporting procedure following loss of CENTRAL data or hardware.

	Don't		**Do**
✗	Don't leave laptops, phones, PDAs, memory sticks, external hard drives or any other processing or storage media unattended.	✓	Do keep mobile and removable devices and media on your person or locked away when you are away from the office. Do lock your office door if you pop out even for just a minute. Do report any losses.
✗	Don't store or process restricted College data or personal data on a non-encrypted mobile or storage device.	✓	Do ensure that any mobile or storage devices on which restricted or personal data are stored or processed are encrypted - items in locked offices can be stolen.
✗	Don't use unencrypted, non-CENTRAL-approved memory sticks to transfer CENTRAL data between workplaces.	✓	Do use a CENTRAL-approved encrypted memory stick.
✗	Don't simply put your encrypted mobile device into sleep mode when it is at risk of theft (e.g. whilst in transit).	✓	Do power your mobile device down fully so that if it is stolen, the data cannot be accessed.
✗	Don't copy the entire College contact directory to your mobile phone.	✓	Do keep the phone numbers of the people you work with most closely. Do delete phone numbers when they are no longer required for work purposes.
✗	Don't store the only copy of data on an encrypted memory stick or on an encrypted hard drive partition.	✓	Do have a securely held backup of data in the event of the encrypted item being lost or stolen or of forgetting the encryption key.

2.7 Printouts

Remember that the Data Protection Act and College confidentiality policies also relate to printed data and we must take just as much care of printed data as we do of electronic data.

The following list of advice is not exhaustive:

- Use the Print Release system wherever possible when printing confidential documents. In the case of pull printing as used on MFDs, it is deleted after 24 hours. Once printed it is no longer shown as available.
- Don't leave printouts with restricted or sensitive data where they can be easily stolen or read by unauthorised people.
- Keep printouts with restricted or sensitive data locked away securely. Each time you leave your office lock them in a secure filing cabinet or desk drawer. Locking your office door is also a good idea but is not sufficient; lock sensitive data in a drawer too - *otherwise unsecured sensitive data stolen from a locked room has recently been construed as a breach of the Data Protection Act*.
- Do not print out any restricted or sensitive data at home.
- Shred all printouts that include restricted or sensitive data - do not, under any circumstances, put printouts with this type of data for recycling.

2.8 Hardware and data disposal

Deleting files from hard drives and other storage media, including formatting of these drives and media, does not necessarily remove the data. You should be aware of the College's policy for disposal of computer equipment.

Major security problems can occur if old equipment, storage media or hard copies of documents are disposed of in an inappropriate way. It is not just CENTRAL equipment and documents that need to be considered, but also any personal computer, mobile device or storage media that has been used to process or store CENTRAL data and any printout of CENTRAL data that you have made away from work.

How to safely dispose of your mobile device.

	Don't		**Do**
✗	Don't throw out old CDs, memory sticks, floppy disks or other storage media, even if you have formatted them or otherwise deleted the data from them.	✓	Do give these or similar data storage media to your departmental IT Support Staff to dispose of securely.
✗	Don't casually dispose of any personal PC,	✓	Do seek advice from IT Support Helpdesk

	laptop or other data processing device that you have used for processing CENTRAL data, even if you have formatted the hard drive or otherwise deleted the data on it.		before disposal. Do understand the College's regulations about use of non-College owned equipment to process College data.
✗	Don't automatically put all print outs into the recycling bins when the data is no longer required.	✓	Do use the CENTRAL Data Classification Scheme Matrix to identify the classification of printed data. Place print outs including only public or open data in the recycling bins. Shred any paper including confidential, strictly confidential or secret data, even if the data is no longer current - see the box below for further information on shredding.
✗	Don't store data either on computer, storage device or as hard copy when you no longer need it.	✓	Do delete or securely dispose of data when you no longer need it - and don't forget to do the same with any backups you have made. Keeping data is a risk - and data also goes out of date - if you need it later, then get up-to-date data.

2.9 WEEE Disposal Policy

All IT and related equipment to be scrapped is disposed of through our appointed WEEE contractor (Enviroelectronics, Doncaster, South Yorkshire). They provide metal cages to all sites in which equipment to be disposed is stored, and these cages are kept in our local secure storage areas. When filled, we contact the contractors and these cages are then collected for disposal at their location in accordance with WEEE regulations. When they collect full cages, they swap these for empty cages which are then used for further equipment disposals. They produce certificate evidence for Hard Drive destruction **only** which are available for review and download from their website via a customer login. We record the equipment detail being disposed of and then remove any relevant items from the organisations IT asset register within our Manage Engine Service Desk Plus helpdesk system.

2.10 Reporting lost or stolen data/hardware

If you suffer a data loss (or suspect that you may have) you must report the loss without delay to the Data Protection Officer (email: Alison.fletcher@Centralnottingham.ac.uk). In your initial report, do not be too specific about the nature of the loss; make sure you provide contact details and we'll get back to you promptly. If the loss is a result of a crime (for example theft) which involved College property or took place on College premises, you should also report the loss to the College's Security Services.

2.11 Anti-virus

All computers connected to Central College's internal network via remote access or any other technology must use a properly configured, up-to-date operating system and anti-virus software; this includes all personally-owned computers.

College computers are protected using Microsoft System Center Endpoint Protection.

Computers remotely accessing college resources can use any of the Anti-virus solutions provided via StaffNet.

3.0 PROTECT YOURSELF

3.1 Network monitoring

All CENTRAL systems users must read and accept the following warning that will appear when users access CENTRAL systems:

> This computer system is the property of Central College Nottingham and is for authorised use by staff, learners and designated contractors only.
>
> Anyone using the College's computer systems should not expect any information stored or content viewed to remain private.
>
> Any uses of the system and / or files stored may be intercepted, monitored, recorded, copied, reviewed and shared with relevant staff as required under various acts of law including but not limited to:
>
> - Data Protection Act 1998
> - Communications Act 2003
> - Malicious Communications Act 1988
> - Computer Misuse Act 1990
> - Counter-terrorism and Security Act 2015
> - Prevent Duty 2015
>
> By logging on to this system, you consent to such interception, monitoring, recording, copying, reviewing and sharing with relevant staff, taking place. Unauthorised or improper use of this system may result in disciplinary and/or criminal action.
>
> By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. Please tick yes if you consent.
>
> If you do not wish to consent, please tick No. Your computer will log off immediately.

3.2 How can I keep safe when using social networking services?

Social networking services, such as Facebook, MySpace, Friends Reunited, Bebo, Twitter and so on, can be fun. However, always read the *privacy agreement* to see what you are agreeing to - and remember that privacy agreements can change.

Be careful about how much information you disclose about yourself - many of these sites are open to anyone and disclosing personal information could have unwanted results, such as identity theft or "cyberstalking".

You can leave yourself open to being physically burgled by giving too much information away about your current movements and location. If you tell people where you are, that tells the less honest ones where you're not - i.e. at home. See the 'Please Rob Me' website: http://pleaserobme.com

If you decide to meet up with someone you've met online, make sure to meet in a public place - or better still, take a friend along too.

3.3 General advice

Don't reply to spam, whatever the provocation in the message - delete the message.

Be wary of messages purporting to be from your bank, or other organisations with which you have an account, that ask you to enter personal details or to click a on a link - this is likely to be a phishing scam. Generally, if the message is genuine, it will refer to you by name rather than as 'dear valued customer'. Also, remember that **no member of CENTRAL staff will ever ask you for your password**.

If a message tells you that you are a lucky prize winner, ignore it - claiming the 'prize' generally involves having to buy something else, to subscribe to something, or will otherwise require you to give personal information - delete the message

If a message asks you to 'pass this message on', don't - just delete it

If a message tells you that you have been chosen to be the recipient of a huge amount of money that has to be got out of a foreign country by legal means, subterfuge or any other 'interesting' ways, just delete it

4.0 PROTECT YOUR COMPUTER

4.1 College-managed computers

Most College PCs are managed by IT Services. On the majority of these computers, you will not have administration rights - that is you are not able to install software on your computer. If you have administration rights (or are unsure whether you have administration rights or not), seek advice from the IT Support Helpdesk immediately.

If you have administration rights it is *your responsibility* to make sure that it is not compromised - remember, if software can be installed on your computer, then so can malware. The ideal advice is to arrange to get your PC properly managed by IT Services.

If you think that your computer has been compromised, there are several things that you must do - refer to IS advice on what to do in case of compromise.

4.2 Your own computer (whether on-site or off-site)

- Make sure that have anti-virus, firewall and anti-spyware software installed
- Make sure that all software on your computer has the most up-to-date patches and updates installed
- Password-protect your computer with a strong password and encrypt any sensitive or personal data
- Make sure that your data is backed up in case of disaster
- Prevent theft or loss of your computer, storage and data
- If using Microsoft XP or earlier version, know the dangers of running your computer with administration rights
- Make sure that removable media are virus-free and kept safe
- Make sure that any handheld devices are secure
- Keep non-Windows computers secure

4.3 **Back up your data**

Remember - you must not process any confidential or higher level CENTRAL data on a non-CENTRAL computer or store it on a non-CENTRAL storage device. If in doubt about data, seek advice from the IT Support Helpdesk.

Question	Answer
How often should I backup my data?	• If it would be a disaster to lose everything from the last week, then backup more frequently than once a week. If it would be a disaster to lose everything from the last day, then backup more frequently than once a day. • You could also create a monthly archive to external hard drive or other storage media. Apart from providing another backup, this also provides a snapshot of work done, which might be useful for audit purposes (for staff) or for documenting learning (for student dissertations and research projects).
What do I need to back up?	• Anything you consider important or which cannot be easily replaced: for example, your academic work, digital photos and music, work saved to your local computer, etc. • Applications do not need to be backed-up as these can be re-installed from the original CDs or from the Internet. You can normally reinstall Windows using the 'System recovery CD' supplied by your computer manufacturer.
What media should I use?	• The best storage device for backup is an external hard drive. Being external, they can be stored away from your computer, which is useful if your computer is damaged or stolen. Cheaper, lower capacity alternatives include USB memory sticks, CDs and DVDs. • There are also external data storage providers, but bear in mind that there may be cost and/or security implications in using these services. Staff, depending on type of data, should seek advice from their local Data Protection Officer.
Where should I store backups?	• Keep multiple backups in different locations but, if they contain sensitive or personal data, make sure that all are kept secure. Staff, depending on type of data, should seek advice from their local Data Protection Officer.
What if I don't backup my data?	• Data recovery is possible, but is expensive and recovery of your data is not guaranteed.

4.4 Prevent theft or loss

Make sure that you know the reporting procedure following loss of CENTRAL data or hardware.

Apart from succumbing to viruses and spyware, there are other ways in which you can lose your hardware and data: for example, your computer or storage media can be *damaged, stolen* or *lost*.

Do not cover your computer or components with anything and switch off your computer when not using it to prevent possible damage through overheating (and to save electricity)

Do not place drinks where they can be accidentally knocked over onto your computer

Update peripheral components and storage media, which degrade over time

Remove memory sticks from PCs or laptops when not in use and follow manufacturers' recommendations when using storage media

Lock your door (and close the window) even if only popping out for a minute - most theft is opportunistic

Always take any hardware and storage media with you if the alternative is leaving it in a public place, such as if going to the buffet or lavatory on a train journey

Don't advertise that you have valuable IT equipment at home as this is an incentive to burglary

Similarly, don't advertise when you are going on holiday or otherwise broadcast when the house is going to be empty (remember - don't give too much information away when setting your Out Of Office message)

Plan journeys so that you don't have to rush - the most oft-cited reason for people leaving laptops and handheld devices on trains/ at the airport is that they are in a hurry

Maintain backups so that data is not irretrievably lost

Ensure that backups are stored away from your computer and in a secure place

Don't just ensure that all data is backed-up, but also ensure that all devices encrypted and/or are password protected with strong passwords so that, if stolen or lost, data on the devices cannot be easily accessed.

4.5 Handheld device security

How to safely dispose of your mobile device.

Phones and other mobile devices often contain your personal information, such as email addresses, phone numbers, or your college password. Even with the utmost care and attention, it is very easy to lose mobile devices.

Treat your mobile device like your wallet or purse

Mobile devices are valuable, not just in themselves, but because of the data they can hold. Treat your mobile devices just like you would your wallet/ purse or credit card. Keep them either on your person or, when not using them, lock them away. Don’t leave them lying around and don’t let someone else use your mobile unsupervised unless you trust them.

Remember, if your password is saved on a device, all someone needs, to log-in as yourself and gain access to any confidential data to which you have access, is just a few minutes.

Set a password or pin number to access your device

A well-chosen password or pin number is a deterrent against casual use and abuse. It isn’t complete protection – someone possessing the device can normally get at the contents with a bit of time and determination. However, it is still a useful layer of security which will stop a casual attacker.

Don’t transfer confidential data to your device

Mobile devices are small, portable and very easy to lose, even when you take precautions against this event. Losing the device is a problem, but losing the data on it can be catastrophic. The College has strict policies and legal obligations about processing data off campus to protect against this risk. Don't transfer confidential data to mobile devices unless you have explicit permission from the College Secretary's Office.

If you aren't sure whether data is confidential or not check the Information Security policy, or err on the side of caution and assume it is. For example a person's salary, home address, photograph and medical history are all *Confidential* or *Strictly Confidential* data.

<u>If your mobile device is stolen or lost, change your CENTRAL password as soon as possible, and contact the phone provider</u>

If someone gets hold of your device and your password is stored on it they can read your email, documents and everything else at the College to which you have access. With phones or mobile broadband devices they can also rapidly run up a bill of thousands of pounds.

For CENTRAL owned phones contact IT Support Helpdesk.

Change your CENTRAL password (contact the IT Support Helpdesk if you need help with this).

Does your device contain any data which is rated at *Confidential* or above? If it does, report the incident to the Data Protection Officer.

<u>Wipe each device thoroughly before disposing of it</u>

Don't just throw out or recycle your phone – it will almost certainly contain your own personal data, such as your contacts list.

If your device has ever been used to hold College data then it is particularly important that it is properly wiped (just deleting data isn't sufficient). Ask for advice or turn it over to IT Support Helpdesk staff for secure disposal, even if it is your personally-owned device.

<u>Turn off Bluetooth</u>

Bluetooth is a wireless protocol for exchanging data between devices. It's useful, but can also be a security risk, letting other people nearby access your phone. Only enable Bluetooth when you actually need it, and then disable it again afterwards. It is a sensible precaution and will also extend your battery life.

<u>Install available updates and anti-virus software if available</u>

Manufacturers release updates to fix security problems and add new features. Always install updates when they are available, as it is important that you get the security fixes.

Anti-virus software runs on a system to protect against known viruses. It is essential that all Windows laptops and desktops have up-to-date antivirus software. Viruses for mobile phones are currently very rare so we don't recommend anti-virus software for phones at this stage.

<u>Use encryption software if advised to do so</u>

Encryption software can be a very strong defence against your data falling into the wrong hands, and is essential if using a device to take *confidential* data off the premises.

Unfortunately encryption is not available for many mobile phones. Encryption is a more practical option for Windows laptops and USB memory sticks. For information on encrypting your laptops or memory sticks, contact the IT Service Desk.

4.6 Non-Windows operating system devices

Although the vast majority of security threats are centred on PCs, the Windows environment and Windows-compatible software applications, this does not mean that those using Macs and other operating systems are safe, just safer. Ensure you adhere to the following (whether on-site or off-site):

- Make sure that have anti-virus, firewall and anti-spyware software installed
- Make sure that all software on your computer has the most up-to-date patches and updates installed
- Password-protect your computer with a strong password and encrypt any sensitive or personal data
- Make sure that your data is backed up in case of disaster
- Prevent theft or loss of your computer, storage and data
- Make sure that removable media are virus-free and kept safe
- Make sure that any handheld devices are secure
- Keep your computer secure

5.0 SECURITY AWARENESS LINKS

General awareness websites

- The UK Government-sponsored Get Safe Online website
- The UK Government's Cyber Streetwise website and the Cyber Streetwise YouTube video channel
- SANS OUCH! Security Awareness Monthly Newsletters
- SANS Security Awareness Video (changes monthly)
- Google's Stay Safe Online resources (developed in association with The UK's Citizen's Advice Bureau)
- Microsoft's Safety & Security Centre website
- The UK Child Exploitation and Online Protection website

Anti-fraud resources

- The Home Office identity theft website
- The National Identity Fraud Prevention website
- The Action Fraud website
- The Metropolitan Police's identity fraud pages
- Personal credit information is available from the Experian website
- Personal credit information is available from the Equifax website
- Personal credit information is available from Callcredit Check