University of York
Information Services

Protecting information

It's everyone's responsibility

Contents

Introduction - we are all responsible for protecting information 03

The golden rules:

1. Handle all information with care 04
2. Ensure critical data is stored safely 04
3. Think before you send 05
4. Keep passwords safe 05
5. Don't fall for a scam 06
6. Secure your computer and mobile devices 06
7. What you do online has repercussions 07

Information classification 08
Where to seek advice 10

We are all responsible for protecting information

Effective information security is fundamental to the work and reputation of the University. Threats to our information security come from many sources and are increasing in both their complexity and sophistication. The University has a legal duty, supported by policies, processes and resources to ensure that we treat data and information appropriately. It is your responsibility, whatever role you have at the University, to understand and comply with these rules, when handling and using data.

This booklet is designed to help you keep both your own and University information safe. It contains practical advice and best practice hints and tips on keeping information secure, and is written in non-technical language. It also contains further sources of information and details of where you can seek help, support, or advice on any aspect of information security.

Protecting information is everyone's responsibility - make sure you do your bit!

Heidi Fraser-Krauss
Director of Information Services

Golden rule 1. **Handle all information with care**

Most data is lost through human error. Any loss of data can have significant financial and reputational implications for the University.

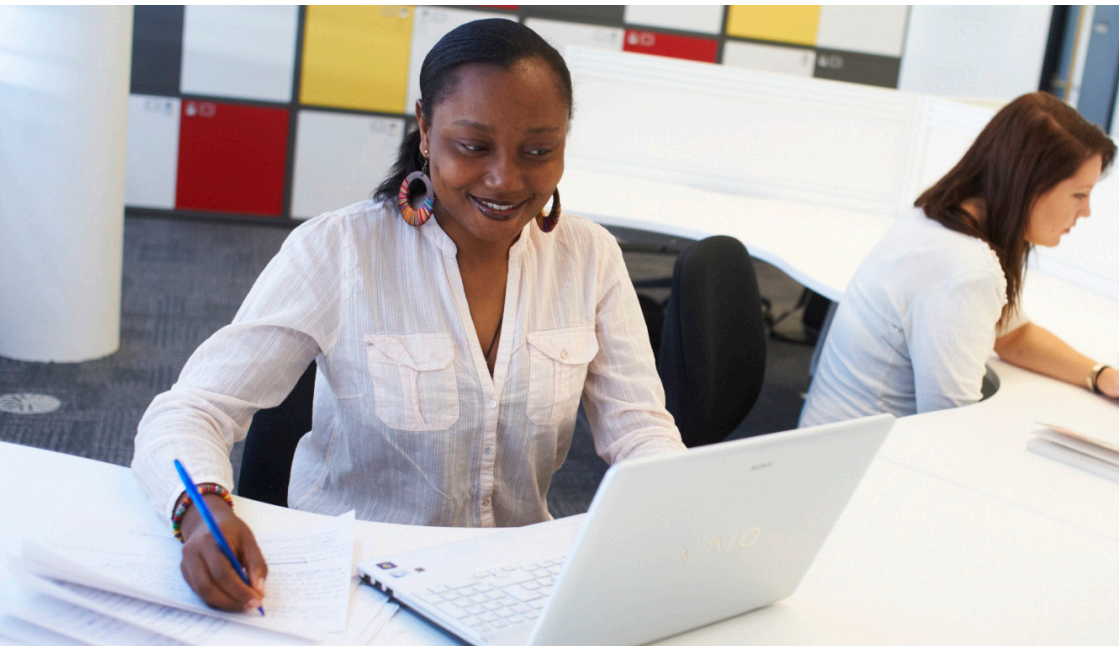
Think carefully about how you collect, handle and share data, and see page 8 for information on how to manage data correctly.

This caution should be applied to all data, whatever its format (eg printed, electronic, hand written). The Data Protection Act places a number of requirements on us related to the handling of personal data - see page 10 for more detail.

Golden rule 2. **Ensure critical data is stored safely**

Data stored in only one place is always vulnerable to loss or corruption. Ensure your data is backed-up and is recoverable. Ideally, use the networked filestores provided by the University or the University's Google Drive service to hold your data.

For critical data, consider making multiple back-up copies in different secure locations.



Golden rule 3. **Think before you send**

Making a mistake when sending email is easy, but it can be a serious issue. The most common way to lose control of confidential data is to email it to the wrong person.

There are three key questions you need to consider before you send:

1. What are you sending?

2. Who are you sending it to and should the recipients know who the other recipients are?

3. Are you sending the right attachment? Is it sensitive? If so, is it protected?

Consider whether you should point the recipient to the document in a secure location (eg the University's Google Drive service or shared filestore) instead of sending an attachment.

Golden rule 4. **Keep your passwords safe**

Passwords are a critical part of your online identity and should not be shared. They provide access not just to the network, but also to your email and networked filestores that may contain personal, sensitive or confidential information such as research data, student records, or salary information.

Never share your password with anyone. IT Services staff will never ask you to reveal your password by email, in person, or on the phone - neither should any other reputable organisation.

Don't use your University IT account password for any other services you use (eg Facebook, Twitter). This minimises the impact if your passwords to other services are discovered.

Password managers

It can be a challenge to keep track of the different passwords required to access websites, services and systems, so we recommend using a password manager.

Find out more about password management at:
www.york.ac.uk/it-services/security/password/

Golden rule 5. **Don't fall for a scam**

Google Mail's spam service stops most spam, phishing and other scam email from reaching your inbox. However, because spammers constantly change the messages they are sending, the first few messages sent in any run will often get through. The messages may ask you to open an attachment, follow a link or reply with personal information.

Be wary of any email or phone call asking you to share personal information - it may be a scam. If in doubt about an email, contact the IT Support Office. If in doubt about a phone call, take the company name and end the phone call without giving out any details - you can check whether it's genuine and call back if necessary.

Golden rule 6. **Secure your computer and other devices**

If your computer, phone or other device gets lost or is infected with a virus, you can easily lose information.

To avoid losing your device, don't leave it unattended. Always use a screen lock to minimise problems if it is lost.

To avoid virus infection, always keep software up to date, and ensure you have anti-virus protection. When you're using your computer, you may see pop-ups asking you to install a new piece of software, accept a download, or similar. Stop and assess what you're being asked to do - if you say no now, you can always change your mind later.

If you are using any device (eg a phone, laptop or tablet) to store or share confidential data, it **must be encrypted** in case of loss or theft. See pages 8-9 for more details about the Information Classification scheme, and see below for information about encryption.

Encryption

Encryption is an important tool to help you protect confidential data.

For advice, please see: **www.york.ac.uk/it-services/security/encryption**

To arrange to have your laptop encrypted, please contact the IT Support Office.

Golden rule 7. **What you do online has repercussions**

When online, treat others as you would in person. Ensure that the language and tone of all communications are appropriate.

Do not post or publish anything that could be offensive or bring the University's name into disrepute. Remember that emails or documents containing personal data may be requested by the individual concerned as a Subject Access Request under the Data Protection Act 1998 (see page 10).

Staff and student disciplinary procedures may be invoked in cases of inappropriate use. If illegal activities are found, external law enforcement agencies will become involved.

Information classification

The University has a classification scheme for all types of information. The aim of the classification scheme is to:

- protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence
- help to meet legal, ethical and statutory obligations
- protect the interests of all those who have dealings with the University and about whom it may hold information (including its staff, students, alumni, funders, collaborators, business partners, supporters etc).
- promote good practice in relation to information handling

The classification scheme encompasses all data held by the University, in any format (electronic and hard-copy). The scheme has three levels:

Public

- This is information which does not require protection and is considered 'open' or 'unclassified' and which may be seen by anyone whether directly linked with the University or not
- Examples include prospectuses, publicity information, open content on the website

Restricted

- Non-confidential information where dissemination is restricted in some way eg to members of the University, partners, suppliers or affiliates
- Examples include teaching materials, some minutes and procurement documents, online directory

Confidential

- Information which is sensitive in some way because it might be personal data, commercially sensitive or legally privileged, or under embargo before being released at a particular time
- Covers data about an individual, and data about the institution
- Examples include personal details, research data, financial transactions

The Information Classification policy was introduced in 2013/14, and can be viewed in its entirety at: **bit.ly/InfoClassification**

What does this mean for you?

If information is classified as **public**, you can:

- share it freely, without needing to encrypt the data
- publish it without restrictions
- dispose of it via normal file deletion, or paper recycling as appropriate

If information is classified as **restricted**, you can:

- send the information unencrypted via email within the University
- print the information out, and send it via the University's internal mail system
- share the information using University IT facilities, eg Google Drive, shared filestore, the York Wiki Service

If information is classified as **confidential**, you must:

- encrypt data before exchanging it
- share data only using University of York facilities
- avoid making duplicate copies if possible, and include protective marking with the data where copies have to be made
- use secure delivery methods for paper copies of confidential information
- mark paper and electronic copies as confidential, and clearly indicate the intended recipients
- encrypt any device used to store or share confidential data. This may be a laptop that has access to your filestore, a tablet used to access confidential documents on Google Drive, or a phone used to read confidential emails. See page 6 for information about encryption.

To **dispose** of information classified as **restricted** or **confidential** you should:

- use the University secure IT waste disposal service (managed by Estates Services) in accordance with any retention schedule if it's stored electronically
- use the University confidential waste scheme (managed by Estates Services) in accordance with any retention schedule for printed information

Legal information

Copyright

If you wish to use, reproduce or even store copyrighted material, consider:

- Can it be used under the exceptions allowed in copyright legislation?
- Does the University have the necessary licence?
- Do you have the permission of the copyright holder?

You need to be able to answer yes to at least one of these to be able to use the material. For more information on copyright compliance, see:
www.york.ac.uk/records-management/copyright

Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) gives anyone the right to access recorded information held by the University. Requested information is made available except where exemptions apply that permit certain types of information to be withheld. Understanding sensitivities and noting possible exemptions helps ensure sensitive information is identified and protected. If you receive a FOIA request, please contact the University's Records Manager for advice:
www.york.ac.uk/records-management/foi

Data Protection Act

The Data Protection Act 1998 establishes an individual's right to have their personal data protected, balancing this against businesses' legitimate need to collect and process data.

Key principles within the act state that data must be:

- Used legally, fairly and transparently, in line with the reasonable expectations of the data subject
- Obtained for specified, lawful purposes
- Adequate, relevant and not excessive for the intended purpose(s)
- Accurate, kept up to date where necessary, and only retained while it is needed
- Accessible to the subject on request (if you receive a subject access request, please contact the University's Records Manager)
- Protected against unauthorised use, loss, damage, or destruction
- Held within the European Economic Area in most cases

Further detail is available at:
www.york.ac.uk/records-management/dp

Where to seek advice

Never assume something is too trivial to report and don't be afraid to get in touch, even if you think the problem is caused by something you've done - our concern will be to fix the issue for you.

Seek advice from or report issues to:

- IT Services (**www.york.ac.uk/it-services**)
- University Data Protection Officer (**www.york.ac.uk/records-management/dp**)
- The University **Computer Emergency Response Team** who will assist if you think your machine has been attacked by hackers or there is other activity of concern taking place. Contact details are at: **www.york.ac.uk/it-services/security**

Learn more about University Information Policy at:

www.york.ac.uk/information-directorate/information-policy

Photographs:

Cover **Shredded Paper** by PaulSH (Flickr) used under a Creative Commons license
p13 and 11 by Paul Shields
p2, 4, 7 and 9 by John Houlihan johnhoulihan.com
p10 **Shredder** by Sh4rp_i (Flickr) used under a Creative Commons license

Printed on recycled paper.