$@*%!

(**Oops!** - Out of protected spaces)

Stay Safe, Stay Secure, Stay Legal

Designed by The Gatehouse, Design & Print Consultancy at Robert Gordon university

What is Sensitive Data?

YOU are responsible and liable for the data you handle, not your line manager, or the University.

A 'health warning' – what constitutes sensitive data is contextual, for example a single email address may not be sensitive in itself but a list of email addresses may be considered sensitive as it would constitute a 'spamming' (unsolicited emails) risk.

Basically there are three types of sensitive data handled at the University:

Personal Data

Sensitive personal information includes sexuality, disability, race, political affiliation, age, salary, criminal convictions.

Other personal data could include home address or photographs. If an individual can identify themselves uniquely from any set of data this too must be treated as sensitive data.

The Data Protection Act 1998 makes provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

For more information check out the University's Data **Protection Training Course** on **CAMPUSMOODLE** (under Staff Links / Records Management), by clicking on the following link: **http://campusmoodle.rgu.ac.uk** and logging in using your usual network ID and password.

Policy Not Yet in the Public Domain

Your line manager or the Records Management should be able to provide guidance on what is sensitive data.

Commercially Sensitive Data

Any data likely to harm the University commercially if it got into the public domain. This typically includes 'trade' secrets, financial information and intellectual property, it certainly includes research data in the University context.

The Freedom of Information (Scotland) Act 2002 requires public authorities such as the University to adopt a publication scheme which is a means of making information available proactively.

Internal and confidential policy not yet in the public domain.

Internal and confidential policy not yet in the public domain.

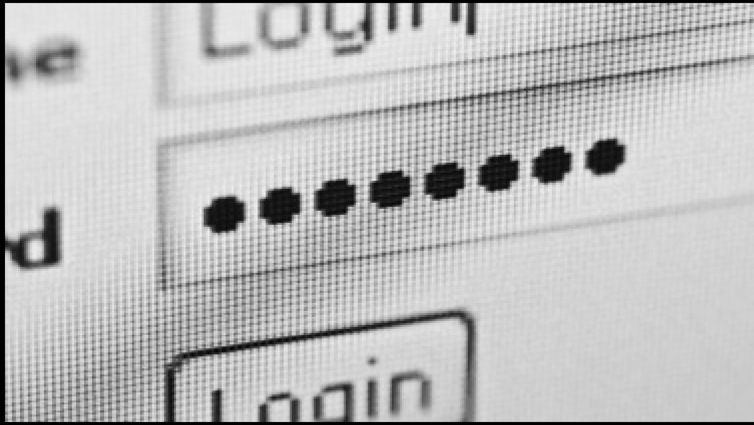
Ensure that you are familiar with the University's regulations for the use of IT.

Related documents and advice are available at **www.tinyurl.com/RGUDPPolicy**

ROBERT GORDON
UNIVERSITY•ABERDEEN

Email and Sensitive Data

Oops!



YOU are responsible and liable for the data you handle, not your line manager, or the University.

Email is not a secure way of transmitting data within the University, so it should not be used to sends sensitive data unless it essential to do so.. A secure way to share data within the University is to use a secure folder on the S Drive and to only email the location of the relevant data.

Who, What, Why and How

If you are about to send sensitive data to someone via email pause and ask:

Who? Who am I sending this to? Am I sending it to the correct address? Is the recipient entitled to see this data?

What? What data am I sending? Is it considered sensitive? Could it be anonymised before sending?

Why? Is there a strong business case for sending this data by email? Could it be made available some other way (e.g., via a secure WEB site)?

How? How do I ensure the data is secure?

If after answering these questions you still need to send the data by email then you should follow this advice.

ROBERT GORDON UNIVERSITY·ABERDEEN

Who?

Check the recipient's email address before hitting the send button. Make sure you do not send sensitive data to the wrong person or persons.

Unless there is a strong business need, sensitive data should not be sent to people outside the University.

What?

Q: What is sensitive data?

A: There are lots of classification systems but use common sense – for instance does the data include personal information? Simply decide if data is either sensitive or non sensitive. Your line manager or Records Management should be able to provide guidance on what is sensitive data. If in doubt, treat as sensitive.

If the data is particularly sensitive, send it as an encrypted attachment rather than the body of the email.

Q: What is encryption?
A: Converting data into a coded form that can not be read without knowing a password or phrase (key).

Why?

Finally, make sure there is a real need to send this data, and if so carry out the checks prescribed here and employ suitable tools to protect the data.

How?

Microsoft Office 2007 and higher provides as standard the ability to encrypt documents to a high level of security. See the Mobile Security Policy at **www.tinyurl.com/MobileSecurityPolicy** for more information. Use **strong complex passwords** which cannot be easily guessed. Passwords should be communicated by telephone or text to the recipient and never by email.

If you are not following these guidelines you should not be sending sensitive data by email.

Handling Sensitive Data

RGU Desktop PC

Oops!

YOU are responsible and liable for the data you handle, not your line manager, or the University.

Here are some general points that if followed should help to keep the Sensitive data you handle on your PC at work secure.

Data Access and Storage

Access to Personal data held by the University should always be accessed through the University's secure systems available via the RGU Desktop.

Personal data must never be stored on your local drives; use Network storage instead.

Passwords

Secure your RGU Workstation with a Password and lock your screen whenever you are away from your desk, and always Logout when you leave for the day.

Never reveal or share passwords. Refrain from writing them down carelessly, if necessary, record them securely.

Emailing Personal Data

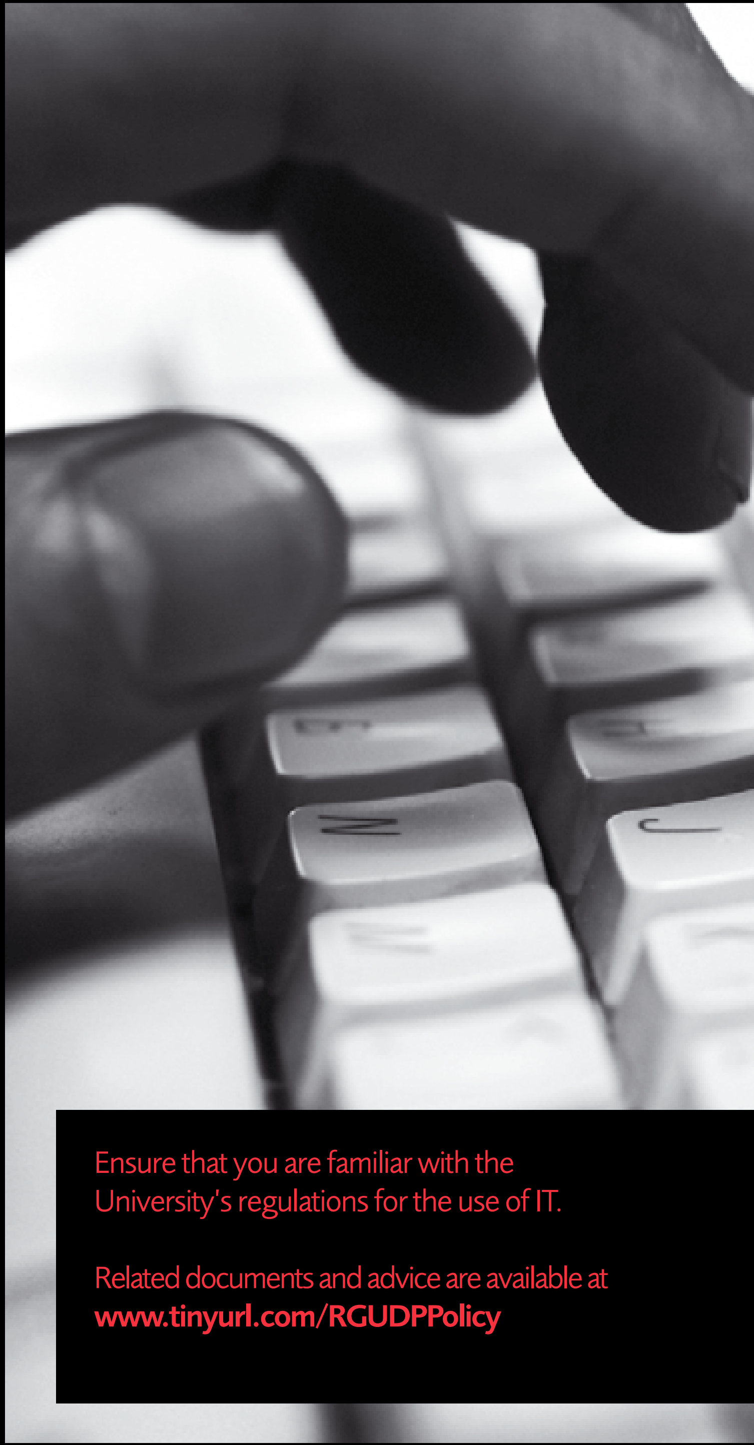
See the **Email and Sensitive Data** Information sheet for guidance.

USB Sticks, CDs, DVDs, Hard Drives etc

All sensitive data held on USB sticks ,CDs etc must be encrypted. See the **Removable Media** information sheet for guidance.

Printouts

Limit printouts to information that is not sensitive.



Ensure that you are familiar with the University's regulations for the use of IT.

Related documents and advice are available at **www.tinyurl.com/RGUDPPolicy**

ROBERT GORDON UNIVERSITY•ABERDEEN

Handling Sensitive Data

Cloud Services

Oops!

YOU are responsible and liable for the data you handle, not your line manager, or the University.

Please note the following points regarding the use of Cloud storage solutions such as iCloud, DropBox, Google Apps etc to store sensitive data.

Data Access and Storage

Cloud services should never be used to store Personal data, even temporarily unless expressly authorised by the Executive Director (IT & Communication).

Personal data should be accessed and processed using the University's secure systems available via its Virtual Desktop, My Apps. **http://myapps.rgu.ac.uk**

Storage of other sensitive data is strongly discouraged.

My Apps should be used wherever possible to access University computer resources Off Campus.

ROBERT GORDON UNIVERSITY•ABERDEEN

Ensure that you are familiar with the University's regulations for the use of IT.

Related documents and advice are available at **www.tinyurl.com/RGUDPPolicy**

Laptop

Oops!

YOU are responsible and liable for the data you handle, not your line manager, or the University.

Here are some general points that if followed should help to keep the Sensitive data you handle on your Laptop secure.

Data Access and Storage

Wherever possible Sensitive Data should always be accessed on a laptop through the University's secure systems via MyApps.**http://myapps.rgu.ac.uk**

Personal data must never be stored on your local drives; use Network storage instead, and where this is not available ensure that all sensitive data (particularly personal data) is encrypted.

Travelling with your laptop

Never leave your laptop unattended – keep it with you.

Secure your Laptop with a robust Password and lock your screen whenever you are away from your Machine.

Avoid using an obvious Laptop bag – they are a target for thieves.

Do not leave your laptop visible in an unattended vehicle, lock it in the boot, or take it with you.

When flying keep your laptop with you as hand luggage.

Use a hotel safe to store your laptop when away from your room.

Removable Media

Oops!

YOU are responsible and liable for the data you handle, not your line manager, or the University.

The majority of serious data breaches involve the loss of removable media such as external hard Drives USB Sticks. Most removable media is easy to lose.

Any sensitive data on mobile media must be encrypted. See the **Mobile Security Policy** at **www.tinyurl.com/MobileSecurityPolicy** for more information.

Data Access and Storage

Don't put sensitive data onto temporary or portable media unless encrypted.

Use an encrypted USB Memory Stick if you need to store sensitive data on a portable device.

Mobile Phone Storage

Do not store sensitive data on your Mobile phone

Activate your Mobile phone's security – check with the IT Help desk for advice about this.

Infection

Data on removable media, such as memory sticks or external hard drives, is potentially at risk every time you plug it to a computer if that computer is infected. Conversely, if removable media is infected, then you run the risk of infecting any unprotected computers that you plug your removable media into, thus putting other users of that computer at risk. Only plug your external devices into protected, trusted computers.

Ensure that you are familiar with the University's regulations for the use of IT.

Related documents and advice are available at **www.tinyurl.com/RGUDPPolicy**

ROBERT GORDON UNIVERSITY·ABERDEEN

Handling Sensitive Data

Smart Phones and Tablet Devices

Oops!

YOU are responsible and liable for the data you handle, not your line manager, or the University.

Users of Smartphones and Tablet Devices such as iPads should be aware of the following security tips:

Security Tips

Protect your device, its information and access to services with a complex Passcode and consider setting it to wipe the contents of your phone after ten consecutive incorrect Passcode entries. Do this right now !

Install updates and security patches regularly.

Only use reputable App stores and check reviews before downloading any software.

Only use trusted and secure Wi-Fi connections.

Set a password on your Voicemail.

Enable the remote wipe function, so if you lose your device you can wipe it . Back up your data regularly – to your PC or a carefully chosen cloud service.

Delete all personal / confidential data before disposing of your device.

Email Access

Using your device's Email application to access your RGU mail may be a convenient way of doing this when you are off campus but ensure that you continue to follow the email guidance when accessing sensitive data.

Always ensure that your device is protected from inappropriate access.

Ensure that you are familiar with the University's regulations for the use of IT.

Related documents and advice are available at **www.tinyurl.com/RGUDPPolicy**

ROBERT GORDON
UNIVERSITY·ABERDEEN

Handling Sensitive Data

Working from Home on your own PC

Oops!

YOU are responsible and liable for the data you handle, not your line manager, or the University.

This guidance applies to all staff who work from home either occasionally or as part of their contract.

Home Computing

Ensure that any processing of personal data at home is covered by the University's Data Protection Policy

Take reasonable steps to protect the information at home from unauthorised loss, access or amendment.

Always work directly from/to the appropriate server using My Apps. **http://myapps.rgu.ac.uk**. This should be used wherever possible to access University computer resources Off Campus.

Ensure that your computer system and applications are up to date with Virus protection software and security patches.

Do not use a non University email account for University business.

Physical Security

Do not take Personal or other sensitive data home, take a copy rather than an official record. Make sure colleagues know that you have it at home.

Security should be of the same standard as that provided by the University.

Take care when transporting information to or from your home, particularly on public transport.

Ensure that you are familiar with the University's regulations for the use of IT.

Related documents and advice are available at **www.tinyurl.com/RGUDPPolicy**

ROBERT GORDON UNIVERSITY•ABERDEEN