Keep in mind…

Where you are and who can hear you when you are discussing a confidential issue with a colleague.

That emails are not always confidential – it is advisable to only include information that you would be happy to be made public.

Who are you emailing? Is it their registered or University account? If you cannot verify the account contacting you is genuine, ask them to resend from their official account (or do not respond).

Where possible, send PDF or un-editable documents. You can password protect your PDF/Office documents before sending them – see the guides at https://staff.bnc.ox.ac.uk/guides

If you have confidential information in your possession, keep it locked away. If the lock on your office door/secure cabinet is not working, inform the relevant person.

Data is more secure stored on a network drive or server than on your local PC. Servers are backed up every 2 hours, 7 days a week and 365 days a year.

Brasenose IT staff are here to help you – if you aren't sure about something or need some help, let us know.

The Brasenose staff website has a guides section containing a selection of tutorials relevant to computer-based staff activities: https://staff.bnc.ox.ac.uk/guides/

Useful University Policies and Guidelines

Brasenose College Staff Policies
https://staff.bnc.ox.ac.uk/policies/

Brasenose Information Security Policy:
https://www.bnc.ox.ac.uk/infosec

University of Oxford Information Security:
https://www.infosec.ox.ac.uk

Tips for Staying Safe Online:
https://www.infosec.ox.ac.uk/i-want

Data Protection:
http://www.admin.ox.ac.uk/dataprotection/

Freedom of Information:
http://www.admin.ox.ac.uk/foi/

Records Management:
http://www.admin.ox.ac.uk/lso/statutes/recordsmanagementpolicy/

Handling of Illegal Material:
https://www.it.ox.ac.uk/policies-and-guidelines/handling-illegal-material

Regulations relating to the use of Information Technology Facilities:
http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

Guidelines for Disposal of Computers:
http://www.it.ox.ac.uk/policies-and-guidelines/computer-disposal

Brasenose College
UNIVERSITY of OXFORD

Brasenose College Information Security Summary

Welcome!

Whether a new starter or existing staff member within Brasenose College it is vital that you recognise the importance of Information Security. We have a duty to protect information entrusted to the College by its members. Otherwise, we risk damaging our reputation and our relationship with those members and many other bodies.

Information classed as personal data (data identifying a living person) is subject to the General Data Protection Regulation (GDPR). A breach of GDPR practices can result in a fine of up to €20 million.

In order to avoid these risks we have developed a College Information Security Policy (ISP) which supports the University of Oxford's ISP. It is essential that you familiarise yourself with both, and ensure you follow protocol and advice at all times.

Remember: If at any stage you suspect personal or confidential data may have been exposed to any person or body that should not have access, it must be reported to your line manager immediately as per the College's Data Breach Policy. Never be afraid to report a breach.

By following these simple fundamental rules you will be avoiding most of the risks posed by poor Information Security. However, you still need to familiarise yourself with the policies.

All staff should complete the University online course on Information Security (SSO Required):

http://www.it.ox.ac.uk/infosec/module

Working with Hard Copies

If copying confidential information, only ever make as many copies as you need, and keep a record of where these copies are and who is using them.

Always remember to check and remove from photocopiers the original document you were copying from.

Delete/destroy/shred copies once they are no longer needed and have been kept for the legal amount of time required (there may be funder-specific regulations, or more general processes).

Shred confidential documents rather than using recycling/waste bins.

Store confidential information in locked cupboards/cabinets.

If this is not possible, store it in a room which is kept locked when unoccupied.

Clearly mark hard copies containing confidential information as 'CONFIDENTIAL'.

If printing confidential documents to a shared printer, ensure you collect them from the printer immediately.

Remember: If at any stage you suspect personal or confidential information may have been exposed to any person or body that should not have had access, it must be reported to your line manger as per the College's Data Breach Policy. Never be afraid to report a breach.

IT Procedures

When requiring access to personal/confidential data offsite it is required to use Remote Access rather than take data offsite.

Permission to transfer/hold personal or confidential data offsite must be requested from the Bursar.

Mobile devices/removable storage should always be encrypted. All devices with access to College email accounts must have a password/PIN lock. Ask IT for help.

Who are you replying to? It is always important to check that any requests for information come from an email address known to be associated with the individual. Where possible, only University email accounts should be responded to. Always double check the 'To' address.

No personal or confidential information should be sent by email or posted to third parties without permission from the Bursar. If permission is given, IT must be consulted regarding the most secure method of transmission.

NEVER share your passphrase with anyone. Try not to use the same password for everything.

Do not leave your computer logged on and unattended – lock the screen when you leave your desk.

Do not follow links or open attachments in unsolicited emails. If in doubt, forward the email to IT. The staff website has guides on spotting Phishing scams.

Permission is required from your line manager if you wish to access your emails on a personal device. The device must be locked with a PIN.

Only visit reputable websites.

If using a personal home computer/laptop for remote access to your College terminal, ensure the operating system and anti-virus are up to date.