REQUIREMENTS

All **information security** incidents must be reported in a timely fashion in order that they are dealt with effectively and efficiently. Incidents should be reported as follows:

- Phishing attacks/emails should be reported to computer.office@bnc.ox.ac.uk
- Report any incidents relating to hard copy only data to data.protection@bnc.ox.ac.uk and your line manager.
- Report all other suspected incidents to your line manager & the College IT Manager.
- If a data breach occurs out of hours or during a holiday period, and if there is a risk the data breach will increase if not addressed immediately, contact the College Lodge who hold emergency contact information.
- If in doubt – report it!

EXAMPLES OF INCIDENTS

- Here are some examples of incidents and who to report them to:

General phishing email targeting financial accounts	college.accountant@bnc.ox.ac.uk computer.office@bnc.ox.ac.uk
Phishing emails targeting University accounts	computer.office@bnc.ox.ac.uk
You have may have responded to a phishing email	computer.office@bnc.ox.ac.uk
Opened an attachment which turned out to be malicious or caused suspicious behaviour	*Ring IT on 01865 275513*
Malware infection on your work machine	*Ring IT on 01865 275513*
Loss or theft of mobile devices	*IT Manager* and line manager.
Loss or theft of hard copy information	data.protection@bnc.ox.ac.uk and your line manager.
Sent an email exposing personal data to the wrong	data.protection@bnc.ox.ac.uk and line manager.

RESPONSIBILITIES

- **Users** are responsible for reporting incidents as per the above requirements.
- **Line Managers** are responsible for ensuring staff are aware of these requirements and for escalating incidents as required in their section.
- **Local IT Support** are responsible for triaging incident reports; confirming incident status; reporting and escalating incidents to appropriate bodies.
- **College Officers** are responsible for ensuring Incidents are recorded and documented. Ensuring incidents are reviewed and subsequent improvements are made to policies and procedures.
- **The Data Protection Officer** is responsible for coordinating the response to, including the escalation of, any breaches of information security affecting personal data.