WADHAM COLLEGE
UNIVERSITY OF OXFORD

Wadham College

Data Breach Procedure

Contents

Revision history

Version	Date	Changes & Approvals
0.1	18 May 2018	Draft for discussion
0.2	24 May 2018	Revisions incorporated
1.0	24 May 2018	Approved for publication
1.1	18 June 2018	Updated contact details

1. Requirements

All information security incidents must be **reported in a timely fashion** in order that they are dealt with effectively and efficiently. The College is required to report **some breaches** to the Information Commissioner's within 72 hours of becoming aware of a breach, and this can take some time to investigate. Incidents should be reported as follows:

- Phishing attacks/emails should be reported to the University InfoSec.
- Report any incidents relating to hard copy only data to data.protection@wadham.ox.ac.uk and the relevant Data Lead.
- Report all other suspected incidents to the relevant Data Lead & 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 Lodge who hold emergency contact information.
- If in doubt – report it!

2. Examples of Incidents

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

General phishing email	phishing@infosec.ox.ac.uk
Phishing email targeting financial accounts	phishing@infosec.ox.ac.uk
Phishing emails targeting University accounts	phishing@infosec.ox.ac.uk
You have may have responded to a phishing email	phishing@infosec.ox.ac.uk
Opened an attachment which turned out to be malicious or caused suspicious behaviour	it-support@wadham.ox.ac.uk
Malware infection on your work machine	it-support@wadham.ox.ac.uk
Loss or theft of mobile devices	it-support@wadham.ox.ac.uk *and* Data Lead
Loss or theft of hard copy information	data.protection@wadham.ox.ac.uk *and* Data Lead
Sent an email exposing personal data to the wrong people	data.protection@wadham.ox.ac.uk *and* Data Lead

3. 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, and for ensuring incidents are reviewed and subsequent improvements are made to policies and procedures.

Data Leads are responsible for information asset registers and Records of Processing Activity in their area.

The *Data Protection Officer* is responsible for coordinating the response to, including the escalation of, any breaches of information security affecting personal data.