Title	Department of Materials Information Security – Incident management		
Document number	ISP004	**Document status**	Approved

Owner	IT Manager (Dr Paul J Warren)
Approver(s)	Department Committee (DC) and IT Committee (ITC)

Version	Version history	Version date
D1	First draft guidance	2021-06-27
D2	Second draft guidance	2021-12-08
D3	Third draft guidance	2022-05-12
V1	Published Version1	2022-05-16

Preface and document control

This document details

This document shall be reviewed at least annually by the IT Committee (ITC) to ensure any new developments are covered and protected.

The master copy can be viewed on the Department of Materials website under “Policies”.

If printed, this document is to be considered “uncontrolled”.

1 Policy on incident management

The university information policy states:

- incidents are effectively managed and resolved, and learnt from to improve our control environment.
- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incident properly investigated and managed;

The departmental information security policy states:

- all information security incidents are reported in a timely manner via appropriate management channels, information systems are isolated, and incidents properly investigated and managed;

2 Responsibilities

- Department of Materials IT Manager is responsible for:
  - ensuring that specific requirements for particular categories of data are recorded in the incident management processes below;
  - ensuring that incidents and activities to resolve them are recorded; *[IT Wiki]*
  - ensuring that incidents are subsequently reviewed; *[reporting to ITC and DC]*
  - implementing improvements to policies and procedures to prevent re-occurrence.
- Line Managers are responsible for:
  - ensuring staff and students are aware of these requirements
  - escalating incidents notified as required.
- IT Support are responsible for:
  - investigating all incidents
  - reporting confirmed incidents to the University within 4 working hours.
- **Everyone is responsible for reporting incidents immediately as per procedures below.**
- The University Information Compliance Team and University Security Team are responsible for coordinating the response to, including the escalation of, any breaches of information security. *[Note that Information Commissioners Office (ICO) requires reporting within 72 hours so every minute counts!]*

3 Incident Response processes

University guidance on incident management is provided at
https://infosec.ox.ac.uk/incident-management

All suspected information security incidents must be reported immediately in order that they are dealt

with effectively and efficiently. If in doubt – report immediately!

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

3.1 Received general phishing email

- General phishing emails not targeting university credentials should not be reported however you may choose to contact the target company (e.g. bank, amazon, ebay etc)
- General phishing emails should be deleted.

3.2 Received phishing email targeting University

- Report phishing attempts targeting University credentials to phishing@infosec.ox.ac.uk and include the original phishing email as an attachment, stating clearly whether you have divulged your credentials or downloaded any attachments. Delete phishing email after reporting.

3.3 Responded to a phishing email targeting University accounts

- If you believe you may have responded to or clicked a link in a phishing email please report immediately to itsupport@materials.ox.ac.uk and include the original phishing email as an attachment, stating clearly whether you have clicked a link or downloaded an attachments or divulged your credentials (in which case you must reset your password). Department IT staff will need to speak to you to clarify details before reporting any confirmed incident to OxCERT within 4 hours. If department IT staff do not respond within 4hrs please contact oxcert@infosec.ox.ac.uk directly.

3.4 Opened an attachment or file leading to malicious or suspicious behaviour

- Please report immediately to itsupport@materials.ox.ac.uk. Department IT staff will need to speak to you to clarify details before reporting any confirmed incident to OxCERT within 4 hours. If department IT staff do not respond within 4hrs please contact oxcert@infosec.ox.ac.uk directly.

3.5 Malware infection or Sophos antivirus alert

- Please report immediately to itsupport@materials.ox.ac.uk. Department IT staff will need to speak to you to clarify details before reporting any confirmed incident to OxCERT within 4 hours. If department IT staff do not respond within 4hrs please contact oxcert@infosec.ox.ac.uk directly.
- All departmental computers should be running Sophos Antivirus which should have on-access scanning running such that it detects known malware and blocks infection, issuing a pop-up alert and sending the alert details to the central console managed by IT staff. Non-

departmental computers (e.g. personal laptops) should also be running Sophos antivirus but alerts will NOT be automatically sent to IT staff so you must report any detection alerts on personal devices to IT staff via email.

3.6 Loss or theft of mobile devices or storage media, e.g. laptops, phones, USB drives

- Loss of an electronic device is usually a data breach and needs reporting immediately. https://compliance.admin.ox.ac.uk/staff-guidance-on-data-breaches
- Please report immediately to data.breach@admin.ox.ac.uk and oxcert@infosec.ox.ac.uk and itsupport@materials.ox.ac.uk and include your line manager. The data breach team will want you to answer the following initial questions.

Circumstances

- 1 - What was the date and time (local) that the device was discovered to be missing?
- 2 - What were the circumstances of the loss? Where was it last seen and how was it secured? What searches have been carried out to find the device (if appropriate)?
- 3 - Have you reported the loss to any other organisation or individual? i.e. police, a lost property department, College wardens, security services. If so please provide details such as who, when, and any relevant reference numbers.

Device Type

- 4 - What kind of device has been compromised?
    - a. Device Type (desktop, laptop, mobile phone, tablet, memory stick etc)
    - b. What is the device make?
    - c. What is the device model and operating system?
- 5 - Is this a University issued device (either through the department or grant etc – please specify) or a personal/other issued device used for University purposes (either occasionally or regularly – please specify)?

Device Security

- 6 - Was the device encrypted? Were there any other security measures configured on the device? Please provide details of encryption (native encryption or OSX/third party encryption product).
- 7 - Was the device secured with a password? If so how robust was the password? I.e. how many characters, and were there any alphanumerical and/or special characters? (**Do not disclose your password to us!**)
- 8 - Does the device have the capability to either 'remote wipe' and/or marked as 'lost or stolen'. If so has this been completed? Please provide details such as action taken, when

action was completed, and what the outcome is.

- 9 - Has the device owner reset their University 'Single Sign On' (SSO) password? Please can you confirm the date (and where possible the time) that this was completed? **NOTE: this must be completed**.
- 10 - Has the device owner reset their University VPN password (where required)? Please can you confirm the date (and where possible the time) that this was completed?
- 11 - What backup arrangements are in place? Is there any information on the device which is now permanently lost? If so – (a) is this personal data and (b) would the loss be detrimental to any individual? I.e. lost the only copy of a student's submitted papers or lost a research participant's consent form.

Data on Device

- 12 - Were University emails accessed via the device? If so was this through:
    - a. Nexus 365 (accessed through web browser);
    - b. Locally installed Outlook;
    - c. Through the University's 'Virtual Private Network' (VPN)
- 13 - Was the device used to access other University apps or systems (i.e. Oracle and CoreHR)? If so was this through a VPN or behind SSO? Please provide details.
- 14 - Would you be able to confirm if any of the following types of personal data (where processed for University purposes not your own personal purposes) were contained on the device or in an email inbox accessed on the device? If so what is the volume of data subjects and volume of data on device (where known or estimated)?
- Please think carefully about this – it may not be immediately obvious but there could be emails or files which contain the below. This can be quite likely where device owners line manage any individuals, supervise any students, or are involved in research trials – if answering yes then please provide context:
    - a. Names, identifiers, and/or contact details (including email and phone)
    - b. Data about mental or physical health of an individual,
    - c. Political, philosophical, religious views of an individual – incl. trade union
    - d. Details about an individual's sex life or sexual orientation,
    - e. Details about an individual's racial or ethnic origin,
    - f. Biometric or Genetic data,
    - g. Criminal Conviction Data (i.e. offences and allegations),
    - h. Any other data considered to be sensitive (i.e. financial or social circumstances)
- 15 - Is the device used for clinical or non-clinical research? If so can you confirm the name

of the trial in question?

- 16 - Were any log on credentials stored on the device or with the device (i.e. post it note)?

3.7 Data breach including GDPR

All data breaches should be reported, but particularly any data breach where the where the confidentiality, integrity, or availability of personal data has been compromised.

- A breach of confidentiality can be defined as where personal data has been exposed/potentially exposed to those for whom it was not intended. *[e.g. misdirected email, incorrect file permissions]*
- A breach of integrity can be defined as where personal data has been wrongly altered and/or mis-recorded.
- A breach of availability can be defined as where personal data has been stolen, lost or wrongly destroyed.

See https://compliance.admin.ox.ac.uk/staff-guidance-on-data-breaches for details.
See https://compliance.admin.ox.ac.uk/examples-of-personal-data-breaches for examples.

Breaches include but are not limited to:

- data breach/loss/theft
- loss or theft of equipment
- inappropriate access controls allowing unauthorised access
- equipment failure
- human error
- unforeseen circumstances such as fire and flood
- hacking
- 'blagging' offences where data is obtained by deception.

It is vital that you report potential personal data breaches immediately when they are discovered. In addition to immediately directly reporting to data.breach@admin.ox.ac.uk (breaches involving personal information) and oxcert@infosec.ox.ac.uk (breaches involving IT security) please also report any breaches to itsupport@materials.ox.ac.uk and your line manager.

The university data breach team will want answers the following initial questions, and will require further email correspondence:

- What happened? (please provide summary description of incident)

- When did the incident happen? (please provide times and dates)
- How and when was the incident discovered? (please provide times, dates, and any reason for a delay in reporting)
- How did the incident occur? Please be as detailed as possible.
- How many individuals have been affected by this incident?
- Are you aware of any adverse effects that have been caused by the incident?
- Have you received any complaints?
- Has the data been recovered or is it still compromised?
- What actions have you taken to contain the incident?
- Have you reported the incident to any other department or organisation (i.e. the law enforcement agencies)?

4 Legal and regulatory requirements

Where incidents may affect the security of particular categories of data, the relevant stakeholders should also be informed. Examples of who to notify in each case are listed below:

Personally identifiable information covered under the Data Protection Act

The Data Protection Act (DPA) is the UK's implementation of the EU's General Data Protection Regulation (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. The university has a data protection policy. Any compromise of personal data needs to be reported to data.breach@admin.ox.ac.uk

Cardholder Data covered under PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. Any compromise of financial cardholder data needs to be reported to cashiers@admin.ox.ac.uk

Generally the Department of Materials does not process cardholder data itself, although it does make use of some central university card payment systems. If in any doubt please report to your line manager and report to departmental IT staff via itsupport@materials.ox.ac.uk and 01865 273727.