Information Management and Policy Services (IMPS)

Information Security Incident Response Procedures

To be read in conjunction with the Information Security Incident Response Policy.

1 Introduction

1.1 The purpose of this document is to provide instruction and guidance on reporting and managing information security incidents. Information security incidents are defined as those involving actual or potential compromise or disclosure of, and/or unauthorised access to, University data to include:

- Sensitive *non* personal data including information of an operational and/or confidential nature, research data, data given in confidence by third parties or data of any kind which is given or the University is required to hold under a contractual confidentiality obligation;
- Personal data (data that identifies living individuals);
- Financial data and/or any information held by the University in respect of it financial or commercial affairs.

1.2 University data includes that which is held on University servers, University hardware and devices (including mobiles, laptops and tablets), and any data pertaining to University business held on personally owned devices. This also extends to University data held externally by a third party on our behalf (including contractors, associates, and partners).

1.3 This document also covers incidences of malicious attacks on University IT, including viruses, malware, ransomware, and denial of service attacks and other threats to the integrity and stability of University data.

If you need to report an Information Security Incident please go to section 2.

For Information on the management of an Information Security Incident, please go to section 3.

2. Reporting an Information Security Incident

2.1 Wherever possible incidents should be reported using the Information Security Incident Reporting Form (Appendix A).

Forms should be completed promptly with as much information as possible and submitted to the address given on the form. Where completion of the form is not possible, the below alternative contacts can be used:

- Potential or actual use of malware, ransomware, denial of service attacks, or breach of IT regulations. Loss or theft of University issued IT including portable devices.

Contact the DTS helpdesk Office Hours 0800-1800 Monday to Friday

on: 0118 378 6262

Email: it@reading.ac.uk

- Potential or actual disclosure or unauthorised access to University data, including personal, sensitive, and confidential data.

  Contact Information Management and Policy Services (IMPS) Office hours 0900-1700 Monday to Friday on:

  0118 378 8981

  Email: imps@reading.ac.uk

- Potential or actual risks posed by physical security, including unauthorised access to buildings, misuse of University identification, suspicious behaviour.

  Contact Security Services (24 Hour)

  0118 378 7799

  Email: securitycontrol@reading.ac.uk

- Out of hours (Friday 18:00 – Monday 08:00)

  For **all** out of hours enquiries contact Security Services

2.2 Due to the potential security risks posed by any further communications in respect of an information security incident, following submission of the form, the details of the incident should remain strictly confidential unless authorisation is given by a Lead Officer.

3 Information Security Incident Management Response

3.1 On receipt of an incident report, the receiving department will notify without delay the following individuals who will act as Lead Officer for the below respective areas:

DTS - Director or Assistant Director (s)

Lead for assessing and responding to risks posed by attacks on University IT networks, misuse of University IT systems, breaches in DTS/IT rules and regulations, and actions required in respect of loss or misuse of University issued mobile devices.

IMPS - Data Protection Officer

Lead for assessing and responding to risks posed by authorised access to and/or disclosure or compromise of personal and sensitive personal data, and data of a commercially or financially sensitive nature.

Security - Security Manager

Lead for assessing and responding to risks posed by physical security compromises, unauthorised access to University property, and reports of suspicious behaviour.

3.2 The above individuals will be responsible for assessing risks posed and further actions required in line with the Incident Response Escalation Process (Appendix B).

3.3 Where the Lead Officer establishes a referral to the Information Security Incident Team (ISIT) is required, the Lead Officer will contact the below designated Lead Officers of the ISIT:

- Data Protection Officer
- Director and/or Assistant Director (s) of DTS
- Director of Legal Services (or alternate)

3.4 The ISIT will then establish if further assistance or notifications are required in line with the Information Security Incident Team: Incident Response (Appendix C). Where necessary, the following Lead Officers will be notified and included in the ISIT:

- DTS staff and specialists
- Business Continuity Officer
- Director of Internal Audit Services (or alternate
- Head of News – Corporate Communications (or alternate)
- Director of HR (or alternate)
- Heads of School, Department or Function
- A relevant member of University Executive Board

3.5 Where the incident involves any suspected criminal activities, the ISIT will designate a Lead Officer to ensure the matter is reported to the Police.

3.6 Where the incident involves personal data, the Lead Officer for IMPS will assess the volume and sensitivity of the data involved and advise the ISIT on whether it is necessary to:

- Inform any affected individuals
- Notify the Information Commissioner's Office

3.7 Where the incident involves non personal information of an otherwise confidential or sensitive nature, for example research data, the Lead Officers for IMPS and Legal Services will assess any contractual or regulatory obligations that may exist in respect of that data and advise the ISIT on whether it is necessary to notify other external third parties or stakeholders.

3.8 Where the ISIT identifies significant risks is respect of either of the above, the incident will be escalated without delay to the University Executive Board, and the Information Systems Managers Group.

4. Review and Monitoring

4.1 Information Security Incident Reports will be centrally recorded and held by IMPS. The record will as a minimum contain:

- Date of the incident and Date Reported
- Reporting persons
- Summary of the Incident, volume and classification of data
- Impact assessment if individuals are affected
- Risk grading (as dictated by IT/Legal/Security departmental assessments)
- Mitigating Actions taken
- Recommendations and further advice

4.2 Information Security Incident Reports analysis and data will be reported into the ISG by the IMPS Officer.

4.3 The ISG will review incidents reported on a quarterly basis to establish if:

- Changes to existing policy is required to improve information management practices;
- additional or improved communications, training or resources for University data users are required to prevent similar occurrences;
- there are patterns of recurring incidents of a similar nature that may suggest high risk areas for priority focus;
- indications are that additional resources are required to reduce the likelihood and severity of future incidents.

4.4 Where necessary, high risk incidents referred to the ISIT will be reported into the Information Systems Managers Group by the ISG.

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0		IMPS	APR 17	UEB	JAN 17	APR 17	APR 18
1.1		IMPS	JAN 21	IMPS	JAN 21	JAN 21	JAN 23

APPENDIX A: SECURITY INCIDENT REPORTING FORM

INFORMATION SECURITY INCIDENT REPORTING FORM

This form should be completed in the event of an actual, suspected or potential Information Security Incident.

This form should be completed in line with the Information Security Incident Response Policy, and as part of the Information Security Incident Procedures.
The effective management of information security incidents is required in order to ensure we meet our obligations under the Data Protection Act, to maintain the security and integrity of the data we hold, as well as being necessary to ensure mitigating and remedial measures can be put in place promptly.

This form can be completed by any member of staff that becomes, or is made, aware of an Information security incident. Students or other non-employees should refer any incidents to a member of staff. This form should be completed as soon as possible, without undue delay, and submitted to the address at the end of the form. In circumstances where completion and submission of this form are not possible, an alternative list of contacts can be found within the Information Security Incident Procedures.

Section 1: Details of Request

1.1 REPORTING PERSONS DETAILS	
Name	Click here to enter text.
Email	Click here to enter text.
School/Department	Click here to enter text.
Contact Number	Click here to enter text.
1.2 INCIDENT DETAILS	
Date of Incident	Click here to enter a date.
Type of Incident	Choose an item.
Does the data at risk include personal or sensitive data (for example names, addresses, emails, financial data)	Choose an item.
Summary of Incident. Please provide details.	Click here to enter text.

Actions taken. Have any mitigating measures already taken to resolve or remedy the incident and/or prevent future occurrences?	Choose an item.	Click here to enter text.

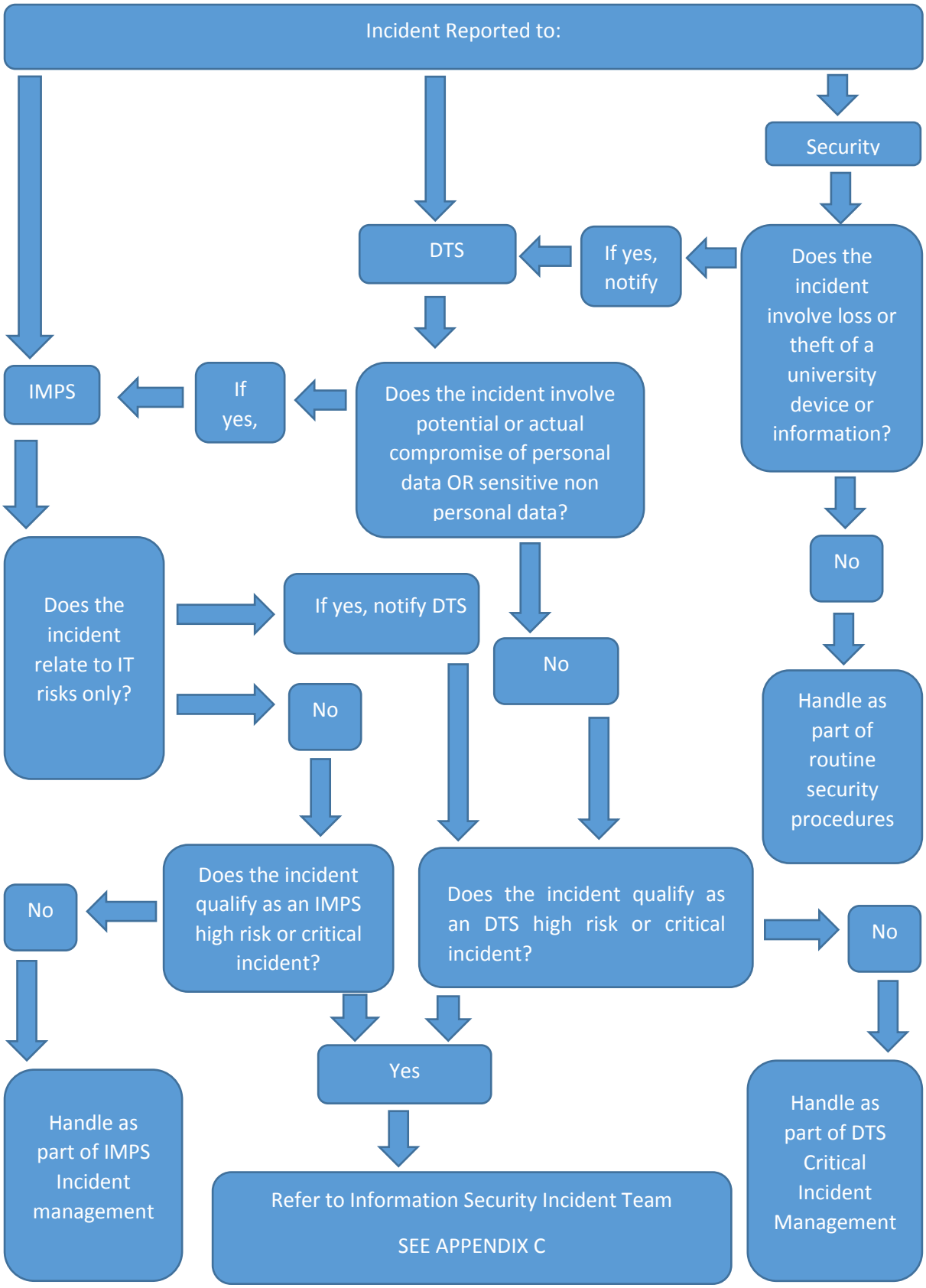
Once completed please return this form to imps@reading.ac.uk

Section 2: IMPS office Use Only

4.2 IMPS OFFICE USE ONLY	
Received on	Click here to enter a date.
Incident Reference Number (IMPS)	Click here to enter text.
Topdesk Ref (if applicable) (IT)	Click here to enter text.
Action Taken	Choose an item.
Date actioned/referred	Click here to enter a date.

Copies of this form to be retained by IMPS for 3 years from date of incident resolution.

APPENDIX B: INCIDENT RESPONSE ESCALATION PROCESS



APPENDIX C: INFORMATION SECURITY INCIDENT TEAM (ISIT) INCIDENT RESPONSE