Information Management and Policy Services (IMPS)

Information Security Incident Response Policy

1. Introduction

To ensure the University can efficiently conduct its business and meet its obligations under Data Protection Laws, the effective and secure management of information is crucial.

All users of University information have a responsibility to:

- complete all mandatory training on Data Protection and Information Security;
- minimise the risk of information being lost or disclosed to unauthorised individuals;
- protect the security and integrity of IT systems or devices on which University information is held or processed;
- ensure that physical security measures for protecting sensitive information are adequate;
- report actual or suspected information security incidents promptly so that appropriate action can be taken to mitigate risks and minimise potential harm to individuals and the University.

2. Purpose

2.1 This policy explains the actions required in the event of an Information Security Incident, and sets out the responsibilities of all users of University data in respect of reporting and managing incidents.

2.2 In the event of an actual (or suspected) information security incident or breach, it is essential that the University takes prompt action to mitigate the risks of potential harm to individuals, damage to operational business, and financial, legal and reputational costs. Where information security incidents are not reported, or where reports are delayed, the consequences can be severe and include:

- damage or disruption to corporate systems;
- damage and distress to individuals;
- monetary penalties from regulators (including very significant fines for breaches of data protection);
- harm to the University's reputation and subsequent erosion of trust;
- loss of business assets;
- increased risk of fraud or identity theft.

3. Scope and definitions

3.1 This policy forms part of the University's Information Framework and has been approved by the Information Security Group (ISG). Overall responsibility for the policy lies with the University Secretary.

3.2 This policy applies to:

i. all information created or received by the University in any format, whether held on campus or remotely, stored on desktop or static devices, or portable devices and media, whether transported from the workplace physically and electronically, or accessed remotely;

ii. any incident that could have a detrimental effect on any University information assets or system;

iii. all users of University information and systems, including staff, students, visitors and contractors working on behalf of the University;

iv. all University owned and managed IT systems;

v. any IT systems on which University information is held or processed, including personally owned devices;

vi. all locations at which University information is held, including non-UK locations.

3.3 An Information Security Incident can be defined as any event that poses a potential, suspected or actual threat to the security, confidentiality, integrity, or availability of University Information. Information Security Incidents can include:

- Intentional or accidental disclosure of any University data, in particular data of a confidential, high risk or sensitive nature of the type set out in section 7 of the encryption policy (www.reading.ac.uk/encryption-policy), to anyone not authorised to view it;
- Loss or theft of paper records, data or equipment such as files, tablets, laptops, or smartphones on which data is stored;
- The execution of a malicious program designed to infiltrate and damage computers without the user's consent (e.g. malware or viruses from clicking on links or attachments in e-mails or from visiting compromised websites);
- Denial of service attacks (e.g. deliberate attempts to interrupt or suspend services of a host connected to the Internet);
- Security attacks on IT equipment systems or networks (e.g. hacking, malware and ransomware);
- Breaches of physical security that pose the threat of unauthorised access to sensitive university information.

3.4 Incidents involving the receipt of spam or 'phishing' emails are also recognised as posing a threat to information security, however, these should be reported via the DTS service Self Service Desk, and do not require the completion of a Security Incident Reporting Form.

4. Roles & Responsibilities

4.1 All users of University Information are responsible for reporting information security incidents. This includes actual, potential, and suspected incidents.

4.2 Heads of School and Functions and Line Managers are responsible for ensuring all users of University information are made aware of this policy, and for assisting with any investigations or incident management response as required.

4.3 The University Secretary has overall responsibility for Information Management and ensuring effective governance of Information Management policies, procedures and training.

4.4 The IMPS Officer (Lead Officer for IMPS) is responsible for: the communication and management of Information Security Incident reports; maintaining a central record of incidents reported and actions taken; advising on mitigations, changes to current practices and making best practice recommendations; co-ordination of incidents referred to the Information Security Incident Team (ISIT), and advising on and completing notifications to the Information Commissioners Office (ICO).

4.5 The Director and Assistant Director (s) of DTS (Lead Officer for DTS) are responsible for assessing Information Security Incident reports referred to DTS, dealing appropriately with those incidents that do not require further escalation, and notifying ISIT where escalation is required.

4.6 The Security Manager (Lead Officer for Security) is responsible for assessing Information Security Incident reports referred to Security, dealing appropriately with those incidents that do not require further escalation, and notifying ISIT where escalation is required.

4.7 The ISIT will have the following core membership:

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

The following members by invitation as required:

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

The ISIT will be responsible for: identifying ISIT members as required; incident containment and recovery; risks assessments and mitigating actions; incident investigations and reports; evaluations of any notifications to information users, regulatory bodies or third parties

required; assessments of current practices and recommendations for change and for reporting into the Information Systems Management Group as required.

5. Policy Procedures

5.1 Information Security Incident Policy, Procedures and reporting mechanisms will be communicated to all relevant personnel and reviewed annually.

5.2 On becoming aware of an Information Security Incident an Information Security Incident Reporting Information Security Incident Reporting Form must be completed and submitted to IMPS. Where completion and/or electronic submission of the form is not possible, alternative contacts will be provided within the Information Security Incident Procedures.

5.3 On receipt of the Incident Report the Lead Officers will make initial assessments, take any immediate remedial actions necessary to contain and recover, and refer to the ISIT if required.

5.4 All reasonable endeavours shall be made to ensure that appropriate technical and organisational measures are taken to ensure the security and integrity of University data. All measures implemented will take into account the sensitivity and volume of data involved, the actual or potential risks posed by the incident, and the operational and business needs of the University.

5.5 All incidents reported will be recorded centrally and maintained by the IMPS Office and made available to Internal Audit on request.

5.6 All incidents referred to the ISIT will be reported to the Information Security Group (ISG) and where necessary reported to the Information Systems Management Group (ISMG).

6. Related policies, procedures, guidelines or regulations

This Policy should read alongside:

Information Security Incident Reporting Procedures.

This policy is related to:

Information Framework Encryption Policy Data Protection Policy

Bring Your Own Device Policy

Information Security Policy IT Regulations

7. Policies superseded by this policy

V0.1, 0.2, 0.3, 0.4, 1.0

8. Review

This Policy shall be reviewed at regular intervals and documented within the version history. Reviews will take place as a minimum at the documented frequency and in the event of any of the below:

- Significant change in University operations
- Significant change in legislation, regulatory requirements, industry guidance or similar
- In the event of a compromise of data protection or security where the content or compliance with this policy is identified as an aggravating or mitigating factor
- Any other identified requirement necessitating substantive changes ahead of scheduled review

Substantive changes shall be reviewed and approved by the Approving Authority as detailed within Document Control.

Un-substantive, minor, or administrative changes may be made by the Policy Owner, or representative of the Policy Owner, as detailed within Document Control.

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
0.1		IMPS	Jan 17	UEB	Jan 17	APRIL 17	Apr 18
0.2	No changes	IMPS	Apr 19	UEB	Apr 19		Apr 20
0.3	IT Services amended to DTS	IMPS	May 20		Apr 20		Apr 21
0.4	No changes	IMPS	Oct 21		Oct 21		Oct 22
1.0	8. Review period updated at CUUP request	IMPS	Oct 22	CUUP	Oct 22	Oct 22	Oct 24
1.1	Reviewed, no changes	IMPS	Oct 24		Oct 24	Nov 24	Nov 26