HERIOT WATT UNIVERSITY

INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURES
MANAGEMENT OF SUSPECTED BREACH OF SECURITY: PERSONAL DATA OR OTHER HIGH RISK INFORMATION

All suspected incidents to be reported to ISHelp@hw.ac.uk
+44 (0) 131 451 4045

IS Help desk team will use the matrix below to route the incident response.

Information Governance (IG) contact details:
+44 (0) 131 451 3219 / 4140 / 3274 / 3218; dataprotection@hw.ac.uk

Type of incident	Lead Officer	Specialist input
Breach of IT security	Global Director of Information Services (IS) or designate	IG: where breach involves loss or compromise of personal data/HIGH risk information
Loss, theft or unauthorised disclosure or modification or destruction of personal data or HIGH RISK information	Head of Information Governance (IG) or designate	Information Services: forensic investigation and chain of custody
Disruption of access to information systems	Global Director of IS or designate	Notify IG
Breach of IT and Communications Facilities Acceptable Use Policy	Global Director of IS or designate	Secretary of the University or designate to approve IS access to user account
Breach of physical security resulting in compromise, loss or theft of devices or equipment; Reporting lost and found devices on campus.	Head of Safeguarding Services or designate: security incidents; lost and found property Global Director of IS or designate: IT issues and lost/stolen devices	IS: remote wiping of device; IG: where breach involves loss or compromise of personal data/HIGH risk information

Confidentiality notice

Information about actual and suspected information security incidents is confidential and must be shared only with staff with designated responsibilities for managing such incidents. Personal data must be shared on a need-to-know basis: only those staff who need this information to deal with the incident and its consequences should know the identity of individual/s involved.

Information security incident management procedures: Personal data or other HIGH RISK information

1 INCIDENT REPORT

For completion by

- IG staff on receiving notification by IS Helpdesk
- Person reporting incident on direction from IG

Please complete this as far as you can on the basis of what you currently know about the incident and send it to dataprotection@hw.ac.uk

If you don’t know the answer it is OK to say so. Don’t wait until you have all the answers to report. It is more important to report potential breaches promptly. Either the Information Governance or Information Services teams will lead the investigation, depending on the nature of the incident, and will ask you for assistance where needed**.**

Date and time of incident	**Place of incident**

Name of person reporting incident

Contact details: email; telephone/address

Please describe what happened

Please describe how the incident occurred

Who discovered the incident and how did they discover it?

What actions have been taken on discovery of the incident?

Which categories of people has been affected by the incident (categories of data subject)

- ○ Students
- ○ Employees
- ○ Contractors
- ○ Research participants
- ○ Customers
- ○ Prospective students and applicants
- ○ Job applicants

- ○ Alumni
- ○ External stakeholders – please give details
- ○ Other – please give details

What categories of personal data have been affected by the incident? Please highlight all that apply

- ○ Data revealing racial or ethnic origin;
- ○ political opinions;
- ○ religious or other beliefs;
- ○ membership of a trade union;
- ○ sexual life;
- ○ sexual orientation
- ○ gender reassignment
- ○ physical or mental health conditions;
- ○ Basic personal identifiers e.g.name, contact details
- ○ Identification data such as user names and passwords economic and financial data such as credit card numbers or bank account details
- ○ official documents/data such as passports, visas or driving licences or national insurance numbers
- ○ Location data e.g. coordinates
- ○ Genetic or biometric data
- ○ Criminal convictions or alleged offences
- ○ Personal information relating to vulnerable adults and children
- ○ Information about work or study performance, salaries or personal life that would cause significant damage or distress to that person if disclosed

Number of personal data records affected

Number of people (data subjects) affected

Does the incident involve confidential information that is not personal data?

- ○ Unpublished research data
- ○ Unique (the only copy of) research data
- ○ Information received in confidence
- ○ Intellectual property or commercially sensitive information
- ○ Information about high profile/high impact strategy or policy under development
- ○ Information that would compromise security or safety if disclosed
- ○ Other – please give details

For University use

Incident reference number

Received by	**On**
Forwarded for action to	**On**