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 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.

PROCEDURES

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 download and complete this form 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**

PROCEDURES

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

2. WORK BOOK AND REPORTING RECORD

2.1: Incident summary: to be completed by Lead Officer {Head of Information Governance (IG) or designate)	
Name of Lead Officer	Role
Incident reference number	
Summary of the actual or suspected security breach	
Date of incident	
School/s Institutes/Professional Services affected	
People involved in/affected by the incident, (such as staff members, students, contractors, external clients) **Personal data must be shared on a need to know basis: only those staff who need this information to deal with the incident should know the identity of the individual/s concerned.**	

Section 2.2: Managing the incident: who needs to be involved	
Please use this checklist below to assess the severity of the incident and determine whether it should be managed as a HIGH, MEDIUM or LOW Critical Incident.	
High Criticality (RED) Is this a major incident?	**YES/NO**
Does containment and recovery, OR the consequences of the loss OR unavailability of the asset require significant University resource to manage beyond normal operating procedures?	**IF YES:** Inform the Secretary of the University and follow the Major Incident Plan.
IF NO:	
Medium Criticality (AMBER): Is this a serious adverse incident?	**YES/NO**
Do containment and recovery require assistance from designated Officers or specialist support teams outside the business unit? OR Does the breach require a notification to the University's senior managers?	**IF YES:** The Lead Officer will inform the other responsible officers and decide who else needs to assist or be made aware of the breach. **Responsible officers** ▪ Global Director of Information Services or designate ▪ Head of IG ▪ Safeguarding and Resilience Manager ▪ Head of Assurance Services ▪ Head of School, Institute or Service affected by the incident **Others who may need to be involved or assist** ▪ Director of Governance and Legal Services ▪ Academic Registrar ▪ Director of Human Resources Development ▪ Director of Marketing and Communications
IF NO	
Low Criticality (GREEN)	**YES/NO**
Can the consequences of the security breach, loss or unavailability of the asset can be managed within normal operating procedures?	**If YES** • Manage incident with the Head of the relevant School, Institute or Service • Send a report of the incident and investigation to IG at InfoGov@hw.ac.uk, and copy to the following **Responsible officers, as relevant**: ▪ Global Director of Information Services ▪ Safeguarding and Resilience Manager ▪ Head Assurance Services ▪ Head of School, Institute or Service affected by the incident

2.3 Assessing the risks and actions to be taken	
The Lead Officer should liaise with the other responsible officers and information/systems owners to consider the following risk factors when assessing, managing and investigating the incident. This list is not intended to be prescriptive and other relevant factors and issues should be recorded as necessary	
Does the incident need to be reported immediately to the police?	**YES/NO**
Risk Factor	**Details and action required**
Which IT systems, equipment or devices are involved in the security breach?	
What information has been lost or compromised?	
How much information has been lost?	
Is the information unique?	
If the incident involves the loss of a laptop or portable device how recently was the information it held backed up onto central IT systems?	
How important is the information or system to the business process or function? Does it include records of operational, legal or evidential value to the University?	
Is it business-critical? Do users rely on access to this particular information asset or can they use reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable?	
How urgently would access need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service?	
Will the loss or compromise of the information have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	

Is the information bound by any contractual security arrangements e.g. to research sponsors?	
Does the incident involve a breach of IT and Communications Facilities Acceptable Use Policy?	
Is any of the information confidential? Please provide details of any types of information that fall into any of the following categories.	
HIGH RISK personal data	
Special categories of personal information (as defined in Articles 9 and 10 of the General Data Protection Regulation) and under the UK Data Protection Act 2018 relating to an identifiable individual's 1. racial or ethnic origin; 2. political opinions; 3. religious or other beliefs; 4. membership of a trade union; 5. physical or mental health or condition; 6. sexual life; 7. proven or alleged offences, including any legal proceedings and their outcome e.g. a court sentence imposed on the individual	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas	
Personal information relating to vulnerable adults and children	
Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed	
Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline	

Sensitive negotiations which could adversely affect individuals	
Security information that would compromise the safety of individuals if disclosed	
Any other personal information that would cause damage or distress to individuals if disclosed without their consent	
Other categories of "high risk" information	
Unpublished research data that has been received or created under conditions of confidentiality and would, if lost or disclosed, significantly impact on the success of a research project, research income. REF outputs or knowledge transfer	
Information received in confidence e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners	
Information that would substantially prejudice the University's or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed	
Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced	
Information that would compromise the security of buildings, equipment or assets if disclosed	

2.4 Who else needs to be informed and take action?	
Reported to Police?	YES/NO If YES notified By… on [date] Incident ref:
IS or external forensic specialist required to protect chain of evidential custody?	YES/NO If YES: action taken By… on [date]
IS to remotely wipe lost or stolen device?	YES/NO If YES: action taken By… on [date]
Reported to Head of IG and DPO (if not the Lead Officer)	Date
Breach of IT and Communications Facilities Acceptable Use Policy (Secretary of the University or delegate Global Directors IS or GaLS) to authorise access to user account for investigation	YES/NO/ Not applicable If YES: Approved by… on [date] Action taken by…. on [date]
IS deletion of email sent in error? Secretary of the University or delegate (Global Directors IS or GaLS) to authorise access to user account to delete email at request of IG/DPO	YES/NO/ Not applicable If YES: Approved by… on [date] Action taken by…. on [date]
Reported to other internal stakeholders	Details, date

Major risks escalated to Risk and Project Management Strategy Group	NO If YES: Date
For Head of IG use:	
Notification to Information Commissioner's Office. A data breach that is likely to result in a risk to the rights and freedoms of data subjects must be notified to the ICO within 72 hours of discovery.	YES/NO If YES notified on [date]
Rationale for decision	
Notification to data subjects	YES/ If YES notified on [date] By:
Rationale for decision	
Notification to other external, regulator/stakeholders	YES/NO If YES notified on By:
Rationale for decision	
For all cases where data subjects, Police, ICO, or other external, regulator/stakeholders to be notified	Confer with Marketing and Communications and invoke the relevant communication plan. [Use template frameworks pre-approved by Secretary of the University]

2.5 Reviewing the incident
The Responsible Officers should meet to review the incident, ensure that all appropriate actions have been taken to mitigate its impact of the incident and to identify further action needed to reduce the risk of a future breach of this kind
How and why the incident occurred
Actions taken to resolve the incident and manage its impact
Impact of the incident (Operational, financial, legal, liability, reputational)
Risks of other adverse consequences of the incident (Operational, financial, legal, liability, reputational)
Any further remedial actions required to mitigate the impact of the breach
Actions recommended to prevent a repetition of the security breach
Resource implications or adverse impacts, if any, of these actions

2.6 Monitoring and managing risks	
To be completed by Head of IG	
Recorded in incident register	Date
Major risks escalated to Risk and Project Management Strategy Group	YES/NO If YES: Date
Risk register for the relevant School, Institute or Service updated	Date By (officer)
Incident report to Global Information Governance and Data Protection Committee (GIGDPC)	Date
Reviewed by GIGDPC on	Date
Recommendations by GIGDPC to reduce risk or minimise impact:	
Policies, procedures or reporting lines to be clarified or strengthened	
Improvements in security controls	
Training and awareness raising	
Other actions	
Additional investment- resource implications	
Reported to Secretary of the University University Executive	on … by …
Actions agreed on [date]	
Responsible Officers	
Timescale	