Document Reference Number	**UoG/ILS/IS 004**
Date	May 2020
Title	Policy for Managing Information Security Incidents (Including Data Breaches)
Owning Department	Information and Library Services
Version	6.0
Approval Date	04-05-2020
Review Date	03-05-2021
Approving Body	Information Assurance and Security Committee

Executive Summary

- The University is committed to ensuring the security of its information systems and the Personal Data for which it is responsible. This policy will ensure that where incidents occur, they are managed in a way that supports compliance with the University's legal obligations and individuals' rights. All users of University Information and information systems are required to familiarise themselves with and comply with this policy. Definitions of terms are in part 10.0 of the policy.

- An Information Security Breach is an incident that has caused or has the capacity to cause unauthorised disclosure of and/or damage to University Information, information systems or reputation. Examples are in part 4.1 of the policy.

- Some of these incidents may involve Personal Data, in which case these are defined as Personal Data Breaches. Examples are in part 4.1 of the policy.

- Members of staff discovering incidents must report the incident immediately to the IT Service Desk at itservicedesk@gre.ac.uk, extension 7555, also to their Line Manager or another senior manager in the absence of the line manager. Reports of Personal Data breaches must also be reported to compliance@gre.ac.uk. Details should be provided using the Incident Reporting Form. More information on reporting information security incidents is in part 5.0 of the policy.

- An incident management team made up of relevant people in Information and Library Services will investigate and assess the risks involved in the incident and will attempt to contain the incident and/or recover systems or data losses. If the incident relates to personal data, the University's Information Compliance Manager will be involved. An investigation will be started within 24 hours of the incident being discovered, where possible. External bodies (e.g. the Information Commissioner) will be notified if necessary. Data Subjects will be notified if a high risk has been identified. For Significant cyber incidents, the Cyber Security Response Team (CSIRT) will lead the operation for investigating and managing such incidents.

Policy for Managing Information Security Incidents (Including Data Breaches)

1.0 Purpose

1.1 The purpose of this policy is to set out the procedure that should be followed to ensure a consistent and effective approach is in place for managing information security incidents including data breaches.

1.2 Care should be taken to protect information and information systems from incidents (either accidental or deliberate) that could compromise their security. In the event of an information security incident, appropriate actions must be taken to minimise associated risks.

2.0 Scope and Responsibilities

2.1 This policy applies to all University staff, students, contractors and third-party agents handling University Information and information systems.

2.2 All users of University Information and information systems are required to familiarise themselves with and comply with this policy.

2.3 All individuals who access, use or manage the University's Information and information systems are responsible for reporting information security incidents (including data breaches) - see point 5.0.

3.0 Compliance

3.1 The University has an obligation to comply with relevant statutory, legal and contractual requirements. The Policy for Managing Information Security Incidents (Including Data Breaches) and Procedure are part of the Information Security suite of policies, designed to ensure information security incidents are reported promptly and managed properly to mitigate the risks to the confidentiality, integrity and availability of University Information and information systems.

3.2 Failure to adhere to this policy will be addressed through the relevant disciplinary proceedings and third-party contractual clauses (as applicable).

4.0 Definition of an incident

4.1 An incident in the context of this policy is an event that has caused or has the potential to cause unauthorised disclosure of and/or damage to University Information, information systems or reputation.

Examples of an Information Security Breach are:

4.1.1 Accidental loss or theft of sensitive or personal data or equipment on which such data is stored (e.g. loss of paper record, laptop, iPad or USB stick)

4.1.2 Unauthorised or accidental use, access to or modification of data or information systems (including inappropriate access permissions to information systems leading to inappropriate disclosure of information)

4.1.3 Unauthorised or accidental disclosure of sensitive or personal information (email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal data posted onto the website without consent

4.1.4 Damage, destruction or loss of personal data, accidental or unlawful alteration of personal data (e.g. due to equipment failure, or a change or deletion of documents on shared drives or other University systems)

4.1.5 Compromised user accounts (e.g. disclosure of user login details through phishing, sharing, public display or a compromised IT system)

4.1.6 Failed or successful attempts to gain unauthorised access to University information or information systems

4.1.7 Equipment failure resulting in non-availability of information

4.1.8 Malware infection

4.1.9 Unusual or uncontrolled file (such as uncontrolled file encryption) and/or system changes

4.1.10 Inappropriate storage and/or disposal of IT equipment

4.1.11 Disruption to or denial of IT service

4.2 Some of these examples may result in a personal data incident or breach. This is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. While all personal data incidents or breaches are information security incidents, not all information security incidents are necessarily personal data breaches. A personal data breach occurs where information relating to identifiable living individuals is involved.

5.0 Reporting an incident and record-keeping

5.1 It is the responsibility of all information and IT resource users (staff, students, contractors and third-party agents) to report information security incidents as soon as possible to the IT Service Desk at itservicedesk@greenwich.ac.uk and extension 7555, as the primary point of contact, and also report it to the relevant line manager or another senior manager in the absence of their line manager.

5.2 Reports of personal data breaches should be sent without delay to the University's Compliance unit at compliance@gre.ac.uk. Data Protection legislation requires any report to be made to the Information Commissioner's Office (ICO) within 72 hours, and the University Secretary as the University's Data Protection Officer will do this if it is necessary. The University Secretary will also determine whether individual data subjects should be informed about the breach.

5.3 Reports should be an accurate description of the incident, including who is reporting the incident, what type of information the incident relates to, and, if personal data is involved, how many people it may affect and the category of people (staff, student, etc.). Details should be provided using the Incident Reporting Form.

5.4 If a computer system breach has occurred, the Director of Information & Library Services (ILS), the Infrastructure Team and the Information Security and Compliance Manager will be informed by the IT Service Desk.

5.5 The Information Security and Compliance Manager will maintain a log of all information security incidents, which will include all stages of the investigation and outcome. The University's Information Compliance Manager will maintain a log of personal data incidents and breaches, which will include all stages of the investigation and outcome.

6.0 Investigation and Risk Assessment

6.1 The Head of Infrastructure or a nominated individual will prompt the appropriate incident management team made up of staff members responsible for the area relating to the type of incident to investigate it. If the incident relates to personal data, the University's Information Compliance Manager will be involved. An investigation will be started within 24 hours of the incident being discovered, where possible. The Cyber Security Response Team (CSIRT) will lead the operation for investigating and managing significant cybersecurity incidents.

6.2 The investigation will establish the nature of the incident, the type of data involved, and will consider the extent of a system compromise or the sensitivity of the data. A risk assessment will be performed as to what might be the consequences of the incident, for instance, whether access to data or IT services could become disrupted or unavailable.

6.3 Where personal data incidents or breaches are concerned, the risk assessment will consider whether there is a risk to individuals. This risk assessment will consider the nature, sensitivity and volume of personal data involved, and the number of data subjects; the ease of identification of individuals from the data; the category of the data subject, for instance, whether they are a child or a vulnerable person; what might be the consequences of the incident and the severity of the impact this would have and the likelihood of this occurring. These factors will help to determine whether there is a risk and what its magnitude might be. The risk assessment will determine whether the incident should be reported to the ICO and whether data subjects should be informed.

6.4 Evidence to support an investigation will be collected as soon as possible and safeguarded to ensure the integrity of the evidence is preserved for forensics and legal admissibility if applicable.

7.0 Containment and Recovery

7.1 The incident management team will determine the appropriate course of action and the required resources needed to limit the impact of the incident. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

7.2 Appropriate steps will be taken to recover system or data losses and resume normal business operations. This might entail attempting to recover any lost

equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

8.0 External Notification

8.1 The Chief Operating Officer (COO) (for information security incidents) will be notified by the Director of ILS, and the University Secretary (for personal data breaches) will be notified by the University's Information Compliance Manager, following a serious data breach involving large amounts of data, or a significant number of people whose personal data have been breached. The University Secretary will decide based on the seriousness of the breach whether to notify the University Governing Body.

8.2 The COO or the University Secretary will decide to inform any external organisation, such as the police or other appropriate regulatory bodies.

8.3 If a breach involving personal data has occurred, the University Secretary as the University's Data Protection Officer will inform the Information Commissioner's Office (ICO) if necessary, based on the risk assessment which has been undertaken. If this is considered to be a risk to people's rights and freedom (under the General Data Protection Regulation) then the ICO will be informed without undue delay and where feasible no later than 72 hours after the University has become aware of the breach.

8.4 The University will where possible notify individuals whose personal data have been subject to a breach, where a high risk has been identified to those individuals, without undue delay. High-risk situations are likely to include the potential of people suffering significant detrimental effect e.g. discrimination, damage to reputation, financial loss, identity theft, fraud, or any other significant economic or social disadvantage. This will help them to take steps to protect themselves. The notice will include a description of the breach and the steps taken to mitigate the risks.

9.0 Review

9.1 Once the incident is contained, a review of the event will be undertaken by the relevant team or an individual and reported to the COO, University Secretary that and the Director of ILS. The report will detail the cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvements to reduce the likelihood or impact of future incidents.

9.2 Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

10.0 Definitions

Authorised Users (in the context of this policy and related documents)	All users who have been given authorisation to use the University's systems.
Availability	Information and information systems are accessible only to authorised users when required.
Confidentiality	Access to, using and sharing of sensitive or personal information is restricted only to authorised users.
Information	Information is data and recorded knowledge, enabling the University to carry out its business. It can be in any format or medium and can include the content of information systems.
Information Systems	Information processing computers or data communication systems.
Integrity	The preservation of the complete, accurate and validated state of Information.
Personal Data	Personal data relates to living individuals (Data Subjects) who can be identified from it, either directly or indirectly, by one or more factors. It includes expressions of opinion, and intentions towards the individual.
Risk Assessment	A process for identifying and evaluating risks, either to people's rights and freedoms, or the risk of adverse events to a computer system.
Sensitive Data	Personal information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sex life or sexual orientation; or commercial or financial information which would not normally be in the public domain.
Unauthorised	Without a legitimate right.

11.0 Related Policies and Legislation

- Links to the Information Security Policies
- Links to the Information Compliance Policies and Codes of Practice
- Data Protection Legislation
- Privacy and Electronic Communications (EC Directive) Regulations 2003