Data Breach Procedure

HPSource holds and processes, personal data, a valuable asset that needs to be suitably protected.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

Purpose

HPSource is obliged under the Data Protection Act to have in place a Data Protection Policy designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This procedure is to be followed to ensure a consistent and effective approach for managing data breach and information security incidents.

Scope

This procedure relates to all personal and sensitive data held by HPSource regardless of format.

The procedure applies to all staff and volunteers at HPSource.

The objective of this procedure is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Types of Breach

For the purpose of this procedure, data security breaches include both confirmed and suspected incidents.

An incident in the context of this procedure is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sentitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems

- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Reporting an incident

Any individual who accesses, uses or manages personal information at HPSource is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (Behla Hutchinson: behla@hydeparksource.org)

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. See Appendix 1

All staff should be aware that any breach of the Data Protection Act may result in Hyde Park Source's Disciplinary Procedures being instigated.

Containment and Recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

The DPO will inform the Management Committee and an investigation (wherever possible within 24 hours of the breach being discovered / reported) will:

- Establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
- Establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.
- Assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
- Determine the suitable course of action to be taken to ensure a resolution to the incident.

The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

Notification

- In line with GDPR legislation the Information Commissioner's Office (ICO) should be notified (if personal data is involved). Guidance on when and how to notify ICO is available from their website at: www.ico.org.uk

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the University for further information or to ask questions on what has occurred.

The Management Committee must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

Evaluation and response

Once the initial incident is contained, the Management Committee will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored

- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Management Committee.

Appendix: Breach forms

Section 1: **Notification of Data Security Breach (to be completed by person reporting incident)**	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Brief description of incident or details of the information lost:	
Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Signed by Data Protection Officer:	
On (date):	
Section 2: **Assessment of Severity**	
Details of the IT systems, equipment, devices, records involved in the security breach:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for HPSource or third parties?	
How many data subjects are affected?	
HIGH RISK personal data ☒ Sensitive personal data (as defined in the Data Protection Act) relating to a living, identifiable individual's a) racial or ethnic origin;	

b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
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;	
Security information that would compromise the safety of individuals if disclosed.	
Section 3: Action taken	
Action taken	
Date of Action Taken	
Was incident reported to Police?	
Follow up action required/recommended:	
Notification to ICO	
Notification to data subjects	
Notification to other external, regulator/stakeholder	