Personal Data Breach Management Policy

University College of Osteopathy

Core Documentation Cover Page					
Personal Data Breach Management Policy					
Version number	**Dates produced and approved (include committee)**	**Reason for production/ revision**	**Author**	**Location(s)**	**Proposed next review date and approval required**
V1.0	May 2018	Produced to assure compliance with data protection legislation.	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Intranet	May 2020 Or in response to legislative changes
V2.0	Nov 2018 IGSSG	Administrative Amendment to update name of committee from "*Information Security & Governance Committee*" to "*Information Governance & Security Steering Group".*	Data Protection & Freedom of Information Officer	All master versions will be held in: J:\0 Quality Team - Core Documentation Website	May 2020 Or in response to legislative changes
V3.0	Nov 2023 IGSSG	Minor Amendments: Amended title of policy to better reflect the focus on breaches concerning personal data; streamlined policy regarding breach management plan; revised data breach incident form for ease of use.	Data Protection & Freedom of Information Officer	All master versions will be held in: SharePoint - Quality Team Website	Nov 2026 Or in response to legislative changes

Equality Impact	
Positive equality impact (i.e. the policy/procedure/guideline significantly reduces inequalities)	
Neutral equality impact (i.e. no significant effect)	X
Negative equality impact (i.e. increasing inequalities)	

If you have any feedback or suggestions for enhancing this policy, please email your comments to: quality@uco.ac.uk

Personal Data Breach Management Policy

CONTENTS

1. Introduction

1.1 The UCO is dedicated to ensure that the personal data it processes is done so in in line with data protection legislation. However, the UCO recognises that personal data breaches may occur for a number of reasons, including:

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as a fire or flood.
- Hacking attacks.
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

1.2 This policy ensures that the UCO responds and manages personal data breaches responsibly, systematically, robustly and effectively and in line with UK data protection legislation.

2. Scope

2.1 This policy is applicable to all members of the UCO who process personal data ("information users") who should implement this policy when they identify a potential, suspected or confirmed personal data breach.

2.2 This policy applies to all personal data processed by the UCO regardless of format and should be read in conjunction with the UCO's Information Security Policy.

3. Responsibilities

3.1 All information users are responsible for reporting actual, suspected, threatened or potential personal data breach incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent risk of harm to individuals affected.

3.2 Senior Managers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

3.3 The Data Protection and Freedom of Information Officer (DPFIO) will be responsible for overseeing the response and management of personal data security breaches in line with the Personal Data Breach Management Plan set out below.

3.4 The DPFIO shall work with members of the Senior Management Team to respond quickly and appropriately to personal data breach incidents.

4. What is a Personal Data Breach?

4.1 A personal data breach in this context means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data processed by the UCO. This includes breaches that are the result of both accidental and deliberate causes.

4.2 Personal data breaches may include:

- Access to personal data by an unauthorised third party.

- Sending personal data to an incorrect recipient.
- Mobile devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss, destruction, corruption or unauthorised disclosure of personal data.

5. Reporting a Personal Data Breach

5.1 Potential, suspected or confirmed personal data breaches should be reported immediately to the DPFIO (dpfio@uco.ac.uk) using the Personal Data Breach Incident Form (Appendix A).

5.2 The DPFIO will undertake an initial risk assessment of the breach (see Table 1) and advise on containing the breach and actions to take depending on the extent, severity and urgency of the breach.

5.3 Where a potential personal data breach is confirmed, the DPFIO will advise the relevant Senior Management of actions to take to minimise the risk of an actual breach occurring. This may include, for example, staff training or changing a process to keep personal data secure.

5.4 Where a personal data breach is confirmed, the DPFIO will initiate the Personal Data Breach Management Plan.

5.5 The DPFIO will keep a record of all reports of potential, suspected and confirmed personal data breaches which will be noted periodically by the UCO's Information Governance & Security Steering Group (IGSSG) to ensure appropriate oversight in the types and frequency of these incidents for reporting purposes in line with guidance published by the Information Commissioner's Office[1] (ICO).

Table 1: Initial Assessment of Data Security Breach

Severity of Breach	Criteria (one of the following)
Major Breach	• The breach involves data classified as Highly Restricted / Restricted. • The breach is likely to cause harm to individuals affected (for example, risk of fraud or significant distress). • The breach involves more than 1000 individuals. • External third party data is involved. • There are significant or irreversible consequences. • The breach is likely to result in media coverage. • An immediate response is required regardless of whether it is contained or not. • The breach requires a significant response beyond normal operating procedures.
Serious Breach	• The breach involves data classified as Restricted. • The breach is not contained within the UCO. • The breach involves personal data of more than 100 individuals. • A significant inconvenience will be experienced by individuals impacted. • The breach may not yet be contained. • The breach does not require an immediate response. • The response to the breach may require notification to UCO's senior managers.

[1] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

Minor Breach	• The breach involves data classified as Internal Use or Restricted. • The breach involves a small number of individuals (less than 100). • The breach incurs a low risk to the UCO. • Inconvenience may be suffered by individuals impacted. • The breach involves data that is contained / encrypted / password protected. • The breach can be responded to during working hours. ***Examples:*** • An email being sent to a wrong recipient. • Loss of an encrypted mobile device.

6. Personal Data Breach Management Plan

6.1 The UCO will take appropriate action to respond to a personal data breach efficiently in line with the personal data breach management plan set out below.

A) Containment & Recovery

6.2 Following the reporting and initial assessment of a personal data breach the DPFIO shall:

a) Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in containing the breach. For example, isolate or close a compromised section of an IT network, or change access codes of doors or IT equipment and systems.

b) Establish whether there is anything that can be done to recover any lost personal data and limit the risk of harm the breach can cause individuals affected. For example, as well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

c) Inform the policy if a crime has been committed, for example, in cases of theft or cybercrime.

B) Investigation & Risk Assessment

6.3 The DPFIO will liaise with the individual reporting the breach and the relevant Senior Manager to fully investigate the breach to determine and confirm the extent and severity of the breach and to identify and take corrective action to prevent any further breach of personal data.

6.4 Once the extent and severity of the breach has been determined, a risk assessment of the consequences of the breach will be undertaken to determine the risk of harm to individuals affected and the likelihood of potential adverse consequences. The risk assessment will be used to inform who is notified of the breach.

C) Notification of a Personal Data Breach

6.5 Where the risk assessment of the personal data breach determines that individuals affected may be at risk of harm, they will be notified in writing without undue delay (Appendix C). The notification will identify what happened, the personal data compromised, what action has been taken to manage the breach and mitigate adverse effects, and information that will enable individuals to protect themselves, for example, a recommendation to change a password for an account, or to remain vigilant for any suspicious activity in a bank account. It will also inform individuals that they may make a complaint to the Information Commissioner's Office and information about how to do this.

6.6 Where the risk to the rights and freedoms of individuals affected is assessed as 'high', the DPFIO will notify the Information Commissioner's Office within 72 hours of becoming aware of the breach, even if all details about the breach have not yet been confirmed.

6.7 Where the risk to the rights and freedoms of individuals affected is assessed as 'high', the DPFIO will also notify any relevant third parties. These may include the Police, banks, and professional, regulatory or statutory bodies, such as the General Osteopathic Council.

6.8 Where the personal data breach is likely to or has come to the attention of the media, the DPFIO will liaise with the Head of Communications & Marketing to draft a press release.

6.9 Where the risk to the rights and freedoms of individuals affected is 'low' or unlikely, the individuals will not normally be notified. Where this is the case, this will be recorded by the DPFIO with the reason why individuals have not been notified.

D) Evaluation & Response

6.10 Further to the investigation, management and response to the personal data breach, the DPFIO and staff involved will identify any enhancements to prevent a similar incident from happening in the future. Actions may include:

- Reviewing the UCO's Information Asset Register and Record of Processing Activity to ensure that personal data processed by the UCO is fully recorded, including what personal data is held, where and how it is stored and how it is transmitted or shared.
- Identifying any present or potential risks and weak points in information security and addressing these.
- Staff training.
- Enhancements to existing or developing new policies.

6.11 The DPFIO shall review any recommended actions to enhance information security and liaise with the appropriate staff members to discuss and implement these actions as appropriate.

6.12 Personal Data Breach Incident Report Forms and recommended actions will be centrally recorded (Appendix B) and considered and monitored by the Information Governance and Security Steering Group (IGSSG) on behalf of the SMT and the Audit & Risk Committee.

APPENDIX A: PERSONAL DATA BREACH REPORT FORM

This form must be completed to report suspected and actual personal data breach incidents.

This form can be completed by anyone with knowledge of the incident.

This form should be completed as soon as a personal data breach has been identified.

Where possible please identify the date and time of events.

Please email the completed form to the Data Protection & Freedom of Information Officer (dpfio@uco.ac.uk) immediately.

INCIDENT DETAILS	
Person reporting the breach:	
Date and time of breach occurring to best of knowledge:	
Nature of breach e.g., theft, disclosed in error, technical problems, etc.:	
Description of how breach occurred:	
Number of people whose data is affected:	
Full description of personal data involved (without identifiers):	
How sensitive is the data?	*Data may be defined as sensitive if it is of a personal nature (such as health records, criminal offence data) or could be misused (such as bank account details).*
How secure is the data?	*Consider whether the data is protected in any way and whether there are safeguards in place to mitigate its loss, e.g., backups or copies.*
Has a formal complaint from any individual affected by this breach been received? If so, provide details:	
Has there been any media coverage of the incident? If so, please provide details:	
INITIAL RISK ASSESSMENT	
Initial risk assessment of breach (to be completed by DPFIO in line with Table 1):	*It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.* *Whether individuals affected are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach.* *Is there a risk to public health or loss of public confidence in an important service the UCO provides?*

CONTAINMENT / RECOVERY	
Containment / recovery action taken including whether and how much the data has been retrieved, contained or remains lost / disclosed:	
As a result of this incident, is any other personal data exposed to similar vulnerabilities? If so, what steps have been taken to address this?	
Is there any evidence to date that the personal data involved in this incident has been inappropriately processed or further disclosed? If so, please provide details:	
What actions have been taken to mitigate risks to individuals' rights and freedoms:	*For example, if individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.*
RISK ASSESSMENT FOLLOWING INVESTIGATION	
Describe the risk to affected individuals' rights and freedoms following investigation of the breach:	*Consider:* *Risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life.* *Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.* *If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.*
NOTIFICATION	
Have all affected individuals been informed? If not, state why.	
Has the ICO been notified? If not, state why:	
Have relevant third parties been notified? If not, state why:	
EVALUATION / RESPONSE	
Identify any weaknesses in the systems, policies or procedures breached either by audit recommendations or anecdotal evidence:	

Have information governance policies and procedures been breached? How? Who?	
Have individuals involved in causing the breach completed regular data protection training? If so, when? If not, why?	
Actions identified for avoiding similar incidents:	

APPENDIX B: PERSONAL DATA BREACH LOG

Ref.	Details of breach					Potential / Actual Consequences of breach	Measures taken/to be taken following implementation of Data Security Breach Management Plan		
	Date of breach	No. people affected	Description of breach	How you became aware of breach	Description of data		Remedial action	Action Responsibility & Deadline	Regulators required to be informed? Provide details.

APPENDIX C: NOTIFICATION OF A DATA BREACH TEMPLATE

Dear <Name>,

This is to inform you that the UCO confirms that a personal data breach has occurred as described below.

We are making every effort to recover the data and to enhance our information security to prevent similar incidences as described below.

Date of data breach:	
What happened:	
What data was involved:	
What the UCO has done to respond to the risks posed by the breach:	
Action you may wish to take to protect yourself further as a result of this breach:	

If you have any questions regarding the above data breach, please do not hesitate to contact me.

Yours faithfully,

XXXX

Data Protection & Freedom of Information Officer (DPFIO)

dpfio@uco.ac.uk

APPENDIX D: PERSONAL DATA BREACH MANAGEMENT FLOWCHART