Data Security Breach Management Policy

University College of Osteopathy

Core Documentation Cover Page					
Data Security 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

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

Data Security Breach Management Policy

CONTENTS

1. Introduction

1.1 The UCO is dedicated to ensure that the data it processes is done so in a secure and appropriate way in line with data protection legislation. However, the UCO recognises that data security 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 data security breaches responsibly, systematically, robustly and effectively.

2. Scope

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

2.2 This policy applies to all information 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 information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

3.2 Senior Managers / Heads of Departments 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 management of data security breaches in line with the Data Security Breach Management Plan; suitable delegation may be appropriate in some circumstances.

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

4. What is a Data Security Breach?

4.1 A data security 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. This includes breaches that are the result of both accidental and deliberate causes.

4.2 Data security breaches involving personal data include:

- Access to personal data by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a data controller or processor.

- Sending personal data to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss, destruction, corruption or unauthorised disclosure of personal data.
- All of the above if it has a significant negative impact on individuals.

4.3 In addition, and as stated within Recital 5 of the GDPR, a personal data breach:

"… may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

5. Reporting a Data Security Breach

5.1 Confirmed or suspected data security breaches should be reported immediately to the DPFIO (dpfio@uco.ac.uk) using the Data Security Breach Incident Report Form (Appendix A). The DPFIO may be contacted to advise on containing the breach and any next steps depending on the extent and urgency of the breach.

5.2 The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved according to the Information Asset Classification System contained within the Information Security Policy by completing the Data Security Breach Incident Report Form (Appendix A) and submitting this to the DPFIO.

5.3 Once a potential, suspected or confirmed data breach has been reported an initial assessment will be undertaken by the DPFIO to establish the severity of the breach in accordance with Table 1 and the Data Security Breach Management Plan shall be initiated.

5.4 The DPFIO shall keep a Personal Data Security Breach Log (Appendix B) to record all reports of confirmed data security breaches to ensure appropriate oversight in the types and frequency of these incidents for management and 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 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.

[1] https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

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.
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. Data Security Breach Management Plan

6.1 The UCO shall take appropriate action to handle a data security breach efficiently utilising its data security breach management plan which consists of the following four elements:

a) Containment and Recovery, where:
- Action is taken to contain and investigate the breach.
- Action is taken to recover data and limit the damage the breach can cause.
- The police are informed if appropriate.

b) Assessment of Ongoing Risk, where:
- A risk assessment is undertaken of the breach and the potential adverse consequences for individuals concerned to determine next steps necessary further to immediate containment.

c) Notification of a Breach, where:
- Individuals concerned, the Information Commissioner's Office (ICO) and third parties are notified of the breach as appropriate depending on the nature of the breach.

d) Evaluation and Response, where:
- The effectiveness of the UCO's response to the breach is considered through action planning and monitoring.
- Improvements to existing procedures are identified to enhance data security.

A) Containment & Recovery

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

a) Identify a member of the Senior Management Team who is independent of the department where the breach occurred to take the lead on investigating the breach.

b) Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise, e.g. isolate or close a compromised section of the network, find a lost piece of equipment or change access codes of doors or IT equipment.

c) Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause, e.g. 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.

d) Where appropriate, inform the pol ice.

6.3 All actions and decisions should be recorded on the Data Security Breach Management Timeline of Appendix A.

B) Assessment of Ongoing Risk

6.4 The lead investigating the data security breach shall undertake a risk assessment associated with the breach to assess potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen using Appendix C to carry out this assessment and to record their findings.

C) Notification of a Data Breach

6.5 The DPFIO and lead investigating the data security breach shall determine whether data subjects or other organisations should be informed of the breach to enable those whose data has been compromised to take steps to protect themselves, to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints using the Notification of a Data Breach Checklist (Appendix D) to determine this.

6.6 If the risk to individuals' rights and freedoms is unlikely, the breach does not have to be reported to the individual or the ICO but shall still be documented in the Personal Data Security Breach Log (Appendix B) by the DPFIO.

i. Notifying Individuals Affected

6.7 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they shall be informed without undue delay. This shall normally by the responsibility of the DPFIO who shall provide individuals affected with the following information using the Notification of a Data Breach template provided in Appendix E:

a) The name and contact details of the DPFIO or other contact point where more information can be obtained.

b) A description of the likely consequences of the personal data breach.

c) A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

6.8 The DPFIO shall record this in the Personal Data Security Breach Log (Appendix B).

ii. NOTIFYING THE ICO

6.9 If a personal data breach has occurred and it has been determined that there is a risk to individuals' rights and freedoms the DPFIO must inform the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, even if all the details have not yet been obtained. This shall normally be the responsibility of the DPFIO who shall follow the ICOs reporting process described here:

https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

6.10 The DPFIO shall record this in the Personal Data Security Breach Log (Appendix B).

iii. NOTIFYING OTHER REGULATORY BODIES

6.11 If the General Osteopathic Council or other regulatory body needs to be informed of a data breach, the DPFIO shall be responsible for providing them with the Notification of a Data Breach (Appendix E).

iv. NOTIFYING THIRD PARTIES

6.12 If third parties, e.g. the police or banks, need to be informed of a data breach, the DPFIO shall be responsible for providing them with the Notification of a Data Breach (Appendix E).

v. NOTIFYING THE MEDIA

6.13 If the data breach is likely to come to the attention of the media, the DPFIO shall liaise with the Head of Communications & Marketing to draft a press release.

D) EVALUATION & RESPONSE

6.14 Further to the investigation of the data breach, the lead member of staff shall identify any enhancements to policies or practices to prevent a similar incident from happening in the future and complete Section 7 of the Data Breach Incident Report Form and provide this to the DPFIO.

6.15 Actions may include:

- Reviewing the UCO's Information Asset Register to ensure that the personal data 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.

6.16 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.

6.17 Data Breach Incident Report Forms and recommended actions shall be considered and monitored by the Information Governance and Security Steering Group (IGSSG) on behalf of the SMT and the Audit & Risk Committee.

APPENDIX A: DATA SECURITY BREACH INCIDENT REPORT FORM

This form must be completed to report suspected and actual data breach incidents such as data loss.

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

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

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

DATA SECURITY BREACH INCIDENT REPORT FORM	
1. SUMMARY OF INCIDENT ***To be completed by the person reporting the data breach.***	
Person reporting the breach:	*Name & Role*
Date and time of incident:	*DD/MM/YY at 00:00*
Number of people whose data is affected:	
Department:	
Nature of breach e.g. theft / disclosed in error / technical problems:	
Description of how breach occurred:	
Signed by the person reporting the breach:	
Date:	
2. REPORTING ***To be completed by the DPFIO.***	
When was the breach reported?	
How did you become aware of the breach?	
Severity of Breach identified by Initial Assessment:	*In accordance with the Initial Assessment as described in Table 1 (delete as applicable):* *a) Major Breach* *b) Serious Breach* *c) Minor Breach*
Who will be leading the investigation of the breach?	*Normally a Senior Management Team member managing an area not involved in the breach.*
Signed by the DPFIO:	
Date:	

3. PERSONAL DATA ***To be completed by the Lead Investigator.***	
Full description of personal data involved (without identifiers):	
Number of individuals affected:	
Have all affected individuals been informed?	
If not, state why not:	
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:	
4. DATA RETRIEVAL ***To be completed by the Lead Investigator.***	
What immediate remedial action was taken?	
Has the data been retrieved or deleted? If yes, state the date and time.	
5. IMPACT ***To be completed by the Lead Investigator.***	
Describe the risk of harm to the individual as a result of this incident:	
Describe the risk of identity fraud as a result of this incident:	
Have you received a formal complaint from any individual affected by this breach? If so, provide details.	
6. MANAGEMENT ***To be completed by the Lead Investigator.***	
Do you consider the employee(s) involved has breached information governance policies and procedures?	
Please inform of any disciplinary action taken in relation to the employee(s) involved.	
Had the employee(s) completed regular data protection training? If so when? If not, why?	

As a result of this incident, do you consider whether any other personal data held may be exposed to similar vulnerabilities? If so, what steps have been taken to address this?	
Has there been any media coverage of the incident? If so, please provide details.	
What further action has been taken to minimise the possibility of a repeat of such an incident? Please provide copies of any internal correspondence regarding any changes in procedure.	
Were you aware of weaknesses in the systems, policies or procedures breached? Either by audit recommendations or anecdotal evidence?	

7. ACTION PLAN

To be completed by the Lead Investigator & DPFIO & monitored by the ISGC

Action	Responsibility	Deadline	Progress

8. TIMELINE

To be completed by the DPFIO & Lead Investigator throughout the investigation.

Date	Time	Action Taken / Decision	Authority
DD/MM/YY	*00:00*	*E.g. Spoke to Department Manager re. breach.*	*Name & Role*

9. SIGN OFF to Confirm Case has been Concluded

To be completed by the DPFIO & monitored by the IGSSG

Completed Date:	
Signed:	
Signed off by IGSSG as all actions completed:	

APPENDIX B: DATA SECURITY 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: ASSESSMENT OF ONGOING RISK

This form should be completed by the senior member of staff identified as the lead on investigating a data security breach.

Senior member of staff identified to lead on investigating the breach:	*Name & Role*
What type of data is involved?	*Describe the data involved in the breach and include the classification of data involved in accordance with the Information Asset Classification System described in the Information Security Policy (delete as applicable):* *a) Highly Restricted* *b) Restricted* *c) Internal Use* *d) Public*
How sensitive is the data?	*E.g. Data may be defined as sensitive if it is of a personal nature (such as health records) or could be misused (such as bank account details).*
What has happened to the data?	*Has the data been lost, damaged or stolen?* *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.*
Is the data involved encrypted or password protected?	*Describe whether the data is protected in any way or were there protection in place to mitigate its loss, e.g. backups or copies?*
What could the data tell a third party about an individual?	*E.g. 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.*
How many individuals' personal data are affected by the breach?	*E.g. 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.*
Who are the individuals whose data has been breached?	*E.g. Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks*
What harm can come to those individuals?	*E.g. Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?*
Are there wider consequences to consider?	*E.g. Is there a risk to public health or loss of public confidence in an important service the UCO provides?*
Who else could help to inform the assessment of ongoing risk?	*E.g. 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.*
Record the date and time that this assessment has been completed on the Data Security Breach Management Timeline in Appendix A.	*See Appendix A.*

APPENDIX D: NOTIFICATION OF A DATA BREACH CHECKLIST

Question	Answer
Has personal data been breached and will this have a significant adverse impact on the individuals affected?	**The individual's affected should be informed without undue delay in accordance with the process outlined in Notifying Individuals Affected.** **The ICO should be informed within 72 hours of the UCO being aware of the personal data breach through their reporting process:** **https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/**
Does the ICO need to be contacted for advice in how to handle the data breach?	*Visit the ICO's website for help:* *https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/*
Are there any legal or contractual requirements to notify individuals or an organisation of a data breach?	*E.g. funding / research contracts? Regulatory body?*
Can notification help us meet our security obligations with regard to the seventh data protection principle?	*E.g. Prevent unauthorised access, loss or damage to the data?*
Can notification help the individual?	*Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?*
Is there a risk of 'over notifying'?	*E.g. Notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.*
Does the notification need to be made appropriate for particular groups of individuals?	*E.g. Children or vulnerable adults?*
Do third parties also need to be notified?	*E.g. the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.*

APPENDIX E: NOTIFICATION OF A DATA BREACH TEMPLATE

Dear <Name>,

This is to inform you that the UCO confirms that a 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 F: DATA SECURITY BREACH MANAGEMENT FLOWCHART