PERSONAL DATA BREACH PROTOCOL

This document must be read in conjunction with Metanoia Institute's (the Institute) Data Protection Policy, IT and Telephone Acceptable Use Policy, Bring Your Own Device Acceptable Use Policy and Disclosing Data to Third Parties guidance.

1. Introduction

1.1. The Institute takes data security very seriously and has procedures and security measures in pace to safeguard against unlawful or unauthorised processing and against accidental loss or damage. By using appropriate technical and organisational measures, every care is taken to protect data from incidents which could result in a personal data breach.

1.2. The focus of this breach protocol is the protection of individuals and their personal data. It has been implemented to ensure that all Institute staff are aware of what a data breach is; and to provide a framework for the containment and management of a breach in order to minimise risk, identify appropriate reporting mechanisms and identify actions to secure personal data and prevent any further breach.

1.3. The protocol applies to all personal data held by the Institute, and to both confirmed and suspected breaches.

1.4. All Institute staff will be made aware of this protocol during induction and may be directed to periodic revisions. All staff are obliged to comply with the protocol at all times.

2. What is a data breach?

2.1. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

2.2. A personal data breach could include (but is not limited to) any of the following:

- loss or theft of personal data or equipment that stores personal data
- inappropriate access controls resulting in unauthorised staff access
- third-party unauthorised use of or access to personal data
- deleting personal data in error
- human error e.g. putting a letter in the wrong envelope, leaving a mobile device containing personal data in transport, etc
- hacking attack
- infection by ransom ware or other instruction on our systems/network
- 'blagging' offences where information is obtained by deception

- destruction or damage to integrity or accuracy of personal data
- equipment or system failure causing personal data to be temporarily unavailable
- unforeseen circumstances e.g. fire, flood or power failure causing personal data to be temporarily unavailable
- inability to restore access to personal data either on temporary or permanent basis; or
- loss of a decryption key where personal data has been encrypted

3. Data breaches by the Institute's data processors

3.1. Where the Institute uses a third-party processor, the requirements for breach reporting are detailed in the contract between the Institute and the processor. This includes a requirement for the processor to inform the Institute without undue delay if it becomes aware of a potential breach.

4. Data breach response plan

4.1. In order for the Institute to contain a breach and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the Institute, all breaches must be reported immediately to the data protection officer (DPO).

4.2. Institute staff may be notified by a third-party (e.g. a supplier that processes personal data on the Institute's behalf) that they have had a breach affecting Institute personal data. Reports of potential data breaches may also be received from individual data subjects, including current and past students. Any member of staff who becomes aware of a potential breach of personal data held by the Institute is responsible for reporting it at the earliest possible opportunity.

4.3. A timely response is critical. The Institute not only has a responsibility to report any breaches to the Information Commissioner with 72 hours of becoming aware of it, it also needs to ensure that it acts without delay in order to protect those individual data subjects involved from any possible adverse consequences of the breach.

Reporting a potential data breach

4.4. Any confirmed or suspected personal data breach which occurs during business hours must be reported regardless of how big or small, or whether or not staff think a breach has occurred or is likely to occur.

In person	NCR Maslow 13 North Common Road Ealing, W5 2QB
By telephone	0208 579 2505 extension 212 0208 832 3083 (direct line)
Via email	dataprotection@metanoia.ac.uk

4.5. Breaches discovered outside working hours must be reported to the DPO as soon as possible.

4.6. Emails should have the subject line "Data Breach Report – URGENT". In the absence of the data protection officer the breach should be reported to the Chief Executive Officer.

4.7. As much of the following information should be provided as possible:

- the data affected;
- how many individuals' records have been affected;
- the current situation – has the breach been contained and if not, how many people could potentially have access to the affected data;
- what action has been taken to resolve the breach;
- how the breach happened;
- when the breach occurred/began;
- any other relevant details.

Stage 1 - Initial Investigation

4.8. An initial investigation into the potential breach will be undertaken by the DPO as soon as the notification is received. This will be used to inform whether an actual breach has occurred, and if so what actions are required to contain it and what formal notification is required.

4.9. The DPO will assess the risks associated with the data involved, taking into account:

- its sensitivity;
- the protection in place e.g. encryptions
- what has happened to the data e.g. has it been lost, corrupted, stolen;
- whether the data could be put to any illegal or inappropriate use;
- who the individuals affected are and the number involved;
- the potential adverse effects of any data subjects e.g. possible identity theft or other fraud, how serious or substantial these are ad how likely they are to occur;
- whether there are any wider consequences to the breach

4.10. Information from the ICO and the Article 29 Working Party guidelines on personal data breach notification will be used to inform the risk assessment process.

4.11. Where it is established that the breach is unlikely to result in a risk to the rights and freedoms of the individuals affected, the incident will be added to the Institute's data breach register and no further action will be taken.

Stage 2 - Containment and recovery

4.12. Where it is established that a data breach has occurred which will impact on the rights and freedoms of the individuals affected, the DPO alongside other relevant Institute staff will:

- determine if the breach is still occurring, and if so appropriate steps will be taken immediately to minimise the effect of the breach;
- 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 inform the police, where appropriate;

4.13. Input and advise from a range of staff across the Institute may be required as part of this process.

Stage 3 - Notification

4.14. Based on the outcome of the initial investigation and with due regard to data protection law and guidance provided by the Information Commissioner the DPO, in consultation with the Chief Executive Officer, will determine who needs to be notified of the breach (see flow chart at appendix A). The Institute may have to notify the ICO and also possibly the individuals affected by the personal data breach. Any notification will be made by the DPO and shall comply with ICO requirements.

4.15. Notification of a personal data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the Institute becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals.

4.16. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, a notification to the individuals affected must be issued without undue delay.

4.17. In any cases where notification to either the ICO or individual data subjects is not required, a detailed record of how the decision was made will be held.

Information Commissioner	
When is notification to ICO required?	Notification to the ICO is mandatory where there is a likely risk to people's rights and freedoms as a result of a breach which could result in physical, material or non-material damage to natural persons such as: • loss of control over their personal data; • limitation of their rights; • discrimination; • identity theft or fraud; • financial loss; • unauthorised reversal of pseudonymisation; • damage to reputation; • loss of confidentiality of personal data; • any other significant economic or social disadvantage to the natural person concerned. Breaches that are unlikely to result in a risk to the rights and freedoms of natural persons do not require notification to the ICO. An example might be where personal data is already publicly available and a disclosure of such data does not constitute a likely risk to the individual. If further investigation uncovers evidence that the security incident was in fact contained and no breach actually occurred, the ICO will be notified. There is no penalty for reporting an incident that ultimately is found not to have been a breach.

Timescale	Without undue delay but no later than 72 hours after the Institute has become aware of the breach. If notification is made after 72 hours, reasons for the delay must be provided. Where full details of the breach are not immediately available, the Institute may notify the ICO in stages. Where this is the case, the Institute will inform the ICO of its intention to provide more information later on and agree with them how and when the additional information should be provided.
How	By contacting the ICO dedicated personal breach helpline on 0303 123 1113. Normal opening hours are Monday to Friday between 9am and 5pm.
What information should be provided?	When reporting a breach the following information will be provided: • a description of the nature of the personal data breach including, where possible; • the categories and approximate number of individuals concerned; • the categories and approximate number of personal data records concerned; • the name and contact details of the data protection officer; • a description of the likely consequences of the personal data breach; • a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Data Subjects	
When should individual data subjects be notified?	If a breach is likely to result in a high risk to the rights and freedoms of individuals they must be informed directly and without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO, not all breaches will be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue. The severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring will be assessed on a case by case basis. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves, particularly if there is a need to mitigate an immediate risk of damage to them. The ICO has the power to compel the Institute to inform affected individuals if they consider there is a high risk. Notification to individuals is not required where: • The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it e.g. state-of-the-art encryption; • Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise e.g. taken action against the individual who has accessed personal data before they were able to do anything with it. • It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.
Timescale	Without delay. In exceptional circumstances where the risk is significantly high this might even take place before notifying the ICO.

How	By transparent and direct communication methods. Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. The Institute will choose a means that maximises the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean employing several methods of communication.
What information should be provided?	The Institute will provide: • A description of the breach in clear and plain language; • The name and contact details of the data protection officer; • A description of the likely consequences of the personal data breach; • A description of the measures taken, or proposed to be taken, to deal with the personal data breach; • Where appropriate the measures taken to mitigate any possible adverse effects; • Where appropriate specific advice on how individuals can protect themselves from possible adverse consequences of the breach, such as resetting passwords.
Chair of Finance, Audit and Risk Subcommittee	The chair of the Finance, Audit and Risk Subcommittee will be informed of any data breaches where notification to the ICO and/or data subjects is required. Where the DPO considers them to be sufficiently serious or indicative of potential systemic issues they will also be informed of any near misses or data breaches which do not require formal notification.
Other authorities	The Institute may also be required to notify third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

5. Evaluation and response

5.1. Once a breach has been contained, the Institute must consider the ongoing risks to the Institute and to any other party and what remedial action can be taken to minimise the impact of the breach.

5.2. The DPO will carry out a detailed review of the causes of the breach, the effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken. The report will be considered by the Institute's Executive Committee, and outcomes shared internally as appropriate.

5.3. A report documenting details of any data breach, the actions and response taken and any lessons learnt will be submitted to the Finance, Audit and Risk Subcommittee for consideration.

Date of Revision	June 2019
Author(s)	Registrar/Data Protection Officer
Date of publication	15 June 2018
Senior Management sponsor	Chief Executive Officer