Data Breach Policy

Contents

1. Introduction

Futura Learning Partnership (the trust) issues this policy to meet the requirements incumbent upon them under the Data Protection Act 2018 for the handling of personal data in its role as a data controller, such personal data is a valuable asset and needs to be suitably protected.

Appropriate measures are implemented to protect personal data from incidents (either deliberately or accidently) to avoid a data protection breach that could compromise security.

A data breach 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.

2. Scope

This policy applies to all employees of Futura Learning Partnership including contract, agency and temporary staff, volunteers, trustees, governors and employees of partner organisations working for the trust.

3. Data Breaches

For the purposes of this policy data breaches will include both suspected and confirmed incidents.

An incident can include, but is not limited to:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*
- Equipment failure (where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- 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 *(e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)*
- Website defacement
- Hacking attack
- Unforeseen circumstances where this leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data) such as a fire or flood
- Human error
- Breaches of policy such as
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss / misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge)*

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back.

4. Risk Assessment and Reporting

The trust encourages open, honest and accurate reporting to minimise impact, improve practice and reduce risk.

The quick response to a suspected or actual data breach is key. When a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, appropriate steps should be promptly taken to address it.

The focus of risk regarding breach reporting is on the potential negative consequences for individuals. On becoming aware of a breach, you should contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

All parties in scope of this policy have a responsibility to report a suspected or actual data breach immediately. If this is discovered or occurs out of hours, this should be reported as soon as practically possible to the person responsible for the management of personal data breaches within the organization (the school's Information Security Lead). This should be done through the completion of the reporting form in Appendix 1, which is sent to the school's Information Security Lead/Headteacher/Principal immediately, who will inform the Chief Operating Officer (COO), and liaise with the trust's Data Protection Officer (i-west). The Chief Operating Officer will, in discussion with the Information Security Lead, appoint an Incident Handler(IH). This may be the Information Security Lead themselves, or another competent person. See Section 5 for further detail.

If the personal data breach is likely to result in a risk to the rights and freedoms of an individual(s), the COO may need to report to the Information Commissioner's Office (ICO), no later than 72 hours after becoming aware of the breach. It is therefore crucial that any data breaches (regardless of the severity) are reported to your Data Protection Officer (DPO) as soon practically possible. It is especially important to report data breaches as promptly where there is low staff availability and or a Bank Holiday. The DPO will advise on whether to notify the ICO, however the final decision will rest with the Chief Operating Officer. If a decision to report is made, then it is the trust's responsibility to liaise with the ICO to ensure the report is sent off.

5. Security Incident Management (SIM)

The Incident Handler (IH) shall complete the following phases of SIM (which are detailed in Appendix 2) with advice from its Data Protection Officer:

a) **Preparation** – the organisation will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches
b) **Identification** – the organisation will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.
c) **Containment & Eradication** – the organisation will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause and inform the Chief Operating Officer immediately. The Chief Operating Officer will establish with the Incident Handler (IH) those who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate. If the breach may include the loss of bank details, notify the trust Finance Department, bank(s) etc of the

potential loss so as to prevent fraudulent uses. In the case of a breach involving the IT system, the Head of IT must also be informed.

Notify data subjects (if necessary) if the breach is likely to result in a high risk to the rights and freedoms of individuals then you should promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach. When notifying individuals, Information Security Leads should consider including the following:

- Outline what has occurred and apologise
- Provide name and contact details of lead officer or relevant manager for further information
- Describe any likely consequences
- Describe any measures taken or proposed to be taken to address the breach including any measures to mitigate its possible adverse effects
- Advise whether the ICO has been notified

Record notification to the data subject in breach log.

d) **Recovery** – the organisation will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.

e) **Wrap Up / Learning from Experience (LfE)** – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. This decision will be taken by the Chief Operating Officer, in consultation with the DPO. The trust's PR consultant may also be notified to handle any queries and release statements. If the IH is not the Information Security Lead, then the outcomes of the investigation will be shared with them.

A review of existing controls will be undertaken by the Chief Operation Officer, in consultation with the DPO, Information Security Lead, and where relevant, the Incident Handler and the trust Head of IT to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Whether policy controls are sufficient
- Whether training and awareness can be amended and/or improved
- Where and how personal data is held and where and how it is stored
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- Whether any data sharing is necessary

If necessary a report recommending any changes to systems, policies and procedures will be considered by the Audit and Risk Committee. This will include the decision on whether to report to the regulator and affected data subjects.

Phases a) to e) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported. Further guidance on this stage can be found in Appendix 3.

6. Monitoring and compliance

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to the Audit and Risk Committee.

Any Data breach which is reported to the ICO will also be reported to the next meeting of the Audit and Risk Committee.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, academy leaders, in consultation with HR, shall have full authority to take the immediate steps considered necessary, including disciplinary action, in line with the trust's Disciplinary policy.

Review this Policy upon:

Change of Data Protection Officer or
Change of Legislation or
Every 3 years, if sooner

Appendix 1 – Data Incident Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	*Please include the name of your school*
Date (and time where possible) of notification to the Information Security Lead/Headteacher	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes.*
2. Recovery of the data	
What have you done to contain the incident?	*eg limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware / informed?	
Have any of the affected individuals made a complaint about the incident?	

Are there any potential consequences and / or adverse effects on the individuals? What steps have been taken / planned to mitigate the effect?	
Your name and contact details:	

Appendix 2 - Security Incident Management (SIM): Record of work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the organisation's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Incident Handler(s) in the organisation (who may be the school's Information Security Lead).

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s)/Information Security Lead):	
Date reported to Headteacher/Principal:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Chief Operating Officer notified (date):	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	• Necessary staff trained on incident handling and incident response • Policy, Procedures & Guidance (link to org policies) • Network Diagrams are held by ICT • The Record of Processing Activities (RoPA) will provide details of data, owners, custodians, and third parties – link to the RoPA • ICT also record event logs and hold logs on other systems (e.g. emails, firewalls etc)

	• Insert any other tools which will help you in incident response • Key contacts: Chief Operating Officer- Tim Howes: vmanuel@futuralearning.co.uk Tel: 0117 9461232 Head of IT- Richard May: rmay@futuralearning.co.uk Headteacher/Principal: initiallastname@schoolname.org.uk
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap Up Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring	

Document the decision to report to both the affected data subjects and the ICO.	
	If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay **Decision to report to Data subjects** - Yes / No Based on: Chief Operating Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - 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 **Decision to report to ICO** - Yes / No Based on: Chief Operating Officer: Signed: Date:

Appendix 3: Further Guidance for the Incident Handler (IH)

1. Investigating a Data Breach

The Incident Handler (IH) shall immediately commence an investigation of the Data Breach.

The IH should consider the type of data, its sensitivity, what protections are in place (eg. encryption), what has happened to the data, how it could be used, how many people are affected by its loss, what type of people have been affected (e.g. pupils, staff, public, suppliers) including their vulnerability and whether, and if so, what are the wider consequences of the breach.

Time is of the essence and, as such, there is a requirement for all investigation to be carried out expeditiously. It is imperative that on notification the DPO along with the IH identify all/any appropriate steps that need to be taken to minimise the impact of the breach. This includes the consideration of how the breach can be recovered and or contained. All agreed actions must be recorded and actioned without delay.

Timescales from realisation of incident	
Notification of incident to the Headteacher/Principal /Information Security Lead and Chief Operating Officer	Without any delay. Immediate consideration by the Chief Operating Officer and recording of actions agreed concerning recovery/containment of the breach
Notification of incident to the DPO by Chief Operating Officer	Without delay
Allocation by Chief Operating Officer to Incident Handler (usually the Information Security Lead)	Without delay
Draft report to DPO (Phase 1 investigation)	As soon as possible but in any case within 24 hours
Data Breach reported to the ICO if reportable	Within 72 hours
Final report (to include completion of Phase 2)	Within 72 hours unless ICO already notified Further time extensions allowed by ICO for complex cases once notified.

2. Investigation Process

An Investigation falls in to two phases:

Phase 1

Immediately establishing/gathering the facts – how, what, why, when and who is affected. This element is time critical. The Incident Handler will need as a minimum to establish the following:

- When the incident occurred (a detailed chronology should be prepared).
- When the data was last seen and when the loss was realised (dates and times)?
- Who was notified of the incident and when, establish how/when they become aware of, or suspected the incident?
- What and whose data has been lost/disclosed, are there any specific issues to be considered – eg. vulnerability?
- How the loss/disclosure happened and why?
- Where the incident occurred (school, other workplace, home, or public place)?
- How many data subjects' information was disclosed?
- Who received the information?
- What is the potential impact on the data subject(s)?
- Was the data subject advised of the disclosure, should they be?
- Assess the risk faced by the individual's whose data has been compromised and how these risks should be managed.
- What was the format of the data (paper, electronic, removable devices)?
- Review any agreed actions taken relating to containment and recovery of the data and determine what, if any further action is required to be taken.

Following the completion of Phase 1 the IH and DPO should assess the risks and based on the information now available the DPO should review all decisions taken and revise accordingly.

Any revisions to the actions/decision must be recorded as part of the IH's report and the DPO should update the original decision log.

The DPO shall also advise at this stage whether the Data Breach requires notification to the ICO and/or other agencies. The decision taken and reasons shall be recorded in the breach log.

Phase 2

a) Assessing potential risks and identifying failures/shortcomings in procedures – what can be done to avoid/minimise the same/similar breach occurring in the future. Issues to be considered will include:

- Was the person who made the disclosure authorised to have access to the data?
- Was the recipient authorised to access this type of data?
- Are there any existing procedures, are they sufficient?
- Were internal procedures followed, if not why not?
- What risks does the trust face as a result of the breach?
- Identify all relevant staff training and guidance and establish whether individuals have undertaken all required training.

b) Developing an Improvement Plan, issues to consider will include:

- Identifying areas for improving systems, processes so as to minimise a repeat of the breach
- Requirements for training,
- Identifiable breaches of adopted trust policies

Stage 2b will be carried out by the Information Security Lead, in consultation with the Incident Handler, the Head of IT (where relevant) and the DPO.

The draft report should be submitted to the Chief Operating Officer immediately on the completion of Phase 1. Submission should not be delayed pending the completion of Phase 2.
The DPO will provide a quality assurance role and ensure that the breach log is updated at relevant intervals.

3. Submission of Final Report (including Improvement Plan)

- It is critical to ensure the trust improves its handling and management of data and as such the preparation of an Improvement Plan following an investigation is an important factor.
- The Information Security Lead should immediately following the completion of Phase 2a of the investigation prepare a draft Improvement Plan, in consultation, where relevant, with the Head of IT, and send this to the DPO.
- The Final Improvement Plan should include any comments made by the DPO in respect of the Improvement Plan, i.e. whether it is accepted or accepted subject to amendments.
- The Final Improvement Report and Improvement Plan should then be submitted to the Chief Operating Officer
- The responsibility for the implementation of the Improvement Plan rests with the trust.