Ox Close Federation

Data Breach Procedure

Approved	**September 2023**
Review Date	**September 2024**

Policy Statement

Schools are responsible for large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is imperative that the appropriate action is taken to minimise any associated risk as soon as possible.

Purpose

This policy sets out the procedure to be followed by Federation staff and Governors when a potential data protection breach takes place. It sets out the decision process by which a potential breach is logged, investigated and a breach determined. The final stages are to decide whether notification of a breach to either the data subjects or the ICO is necessary.

Scope

This procedure applies to all personal and sensitive personal data held by the Federation.

Definitions

Data	A collection of facts from which conclusions may be drawn.
Personal data *(as defined by the Data Protection Act 1998)*	Data that relates to a living individual who can be identified from that data, or from that data and other information that comes into the possession of the Data Controller. For example: ▪ Name ▪ Address and postcode ▪ Date of birth
Special Category Data *(Formerly Sensitive Data)*	Personal data consisting of: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious or similar beliefs ▪ Trade union membership ▪ Physical or mental health or condition ▪ Sexual life ▪ Genetic or Biometric Data
Data Controller	A person or organisation that determines the purposes for which, and the manner in which, personal information is to be processed. The Federation should be registered as a Data Controller.
DPA	Data Protection Act 1998

Data Processor	A person who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition. A Federation employee is not a data processor.
Data Subject	The living individual who is the subject of the data/personal information.
GDPR	General Data Protection Regulation (new European legislation that will supersede the DPA)
LADO	Local Authority Designated Officer
Potential Data Breach	The potential loss, theft, corruption, inappropriate access or sharing of personal, or sensitive personal data.
Phishing / blagging	The act of tricking someone into giving out confidential information.
ICO	Information Commissioner's Office The ICO is the UK's independent public body set up to promote access to official information and protect personal information by promoting good practice, ruling on eligible complaints, providing information to individuals and organisations, and taking appropriate action when the law is broken.
Ransomware	Illegal software that encrypts users' data, then holds the Federation to ransom demanding payment of hundreds of pounds to provide the password.
Schedule 2 conditions (as amended by the GDPR) that may be relevant:	(i) consent (ii) needed for contractual performance (iii) needed to comply with legal obligations (iv) needed to protect vital interests (v) needed to perform a task in the public interest or in the exercise of official authority
Schedule 3 conditions (as amended by the GDPR) that may be relevant:	(i) explicit consent (ii) necessary processing by an employer (iii) to protect vital interests (iv) where the data has been manifestly made public by the subject (v) necessary for judicial proceedings (vi) necessary for substantial public interest reasons (vii) necessary health processing (viii) necessary for archiving purposes
Actionfraud	http://www.actionfraud.police.uk/ National cybercrime reporting centre.

Legal Context

The Data Protection Act regulates the processing (use) of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.

Principle 7 of the Data Protection Act 1998 states that organisations which process personal data must take "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

What is a potential data breach?

A potential data breach occurs, in general, when the Data Protection Act is not complied with in the processing of personal information. What this means is that the failure to comply with any of the 8 data protection principles can be considered a breach. The 8 data protection principles are as follows:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
    - at least one of the conditions in Schedule 2 is met, and
    - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met and the processing is proportionate to the aim pursued and respects the essence of data protection rights.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This Data Breach Procedure aims to ensure that the Federation fulfils the seven Data Protection Principle and takes appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

A potential data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Accidentally sharing data with someone who does not have a right to know this information
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error resulting in data being shared with someone who does not have a right to know
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the Federation to disclose personal information.

Examples of these include:

- The loss or theft of all or part of a service user's personal information, containing identifying information and/or details of their current personal circumstances.
- Sharing of personal and/or sensitive service user information when consent has not been given and there is no legal basis to override this. Or more information is sent than is required. For example, if you send a whole medical file when a sickness absence form is all that is needed.
- Emailing service user personal and/or sensitive personal information outside the Federation without appropriate security encryption measures in place. For example, if you send a case review notes record over an unsecured email system.

The list is indicative but not exhaustive. If you are, in any way, unsure whether or not a potential breach has taken place the Federation's Data Protection Officer should be contacted and legal advice may be sought.

What about an Information Communication Technology (ICT) breach?

If a potential breach involves an ICT device or service, such as a lost laptop, an errant email or a stolen USB stick, then technical advice should be sought from the ICT service provider.

Mandatory Procedures**:**

When a potential breach has occurred, the Federation will need to investigate it to determine if an actual breach has occurred. In that process, there are four steps to manage and investigate a potential breach. They are:

- Reporting
- Containment and Recovery

- Investigating/Managing
- Evaluation and response

For each stage, there is **a key decision.** The following steps set out the decision process at each stage. (See also the flowchart at end of document.)

The report template is included (at the end of the document) to help staff identify and manage potential breaches.

Reporting the Potential Data Breach

Responsible Officer: Data Protection Officer

The first decision stage is to determine whether a potential breach has occurred. If you discover an incident that meets the criteria set out earlier (i.e. breaches any of the criteria set out at paragraph 6 above), you need to start this process.

Keep a log of all potential and investigated breaches. The log can then be analysed to ensure that any lessons learnt from breaches can be implemented.

Record the following in the log if known:

a) Date of incident

b) Date you were made aware of the potential breach

c) Location of incident

d) Nature of incident, that is, is it a loss, theft, disposal, unauthorised disclosure?

e) Nature of data involved, list all data elements. For example, whether it is names, files, dates of birth, or reference numbers

f) What security protection was on the data? Is it protected by a password, encryption, or something else?

g) Is there a backup of the data, if so where?

h) Number of people potentially affected, an estimate should be provided if no precise figure can be given.

i) Details of any steps taken to retrieve data or to contain the breach if it involved unauthorised access or potentially compromised security.

Note: If the incident involves the theft, for example, of a bag containing personal documents or a laptop, the theft must be reported to the Police.

Containment and Recovery

Responsible Officer: Data Protection Officer

The **second decision stage** is to consider whether the potential breach needs an investigation template or whether it can be contained within the Federation. The focus is on whether the potential breach has been contained. If so, this will be logged as a **near miss** and no further action will be taken.

The reasons behind the near miss will be analysed and any trends or learning outcomes will be shared across the services to prevent future breaches.

Worked example.

A teacher contacts the head to say that an envelope containing sensitive personal information about the medical condition of a pupil was given to the wrong Educational Psychologist. The envelope has not been opened and the Federation has been contacted by the Educational Psychology Service. The Federation will need to collect the envelope to secure the information. In this instance the information was contained. This would be recorded as a 'near miss'.

If the breach has not been contained then the Federation should follow the data breach investigation template. A copy of this template at the end of this document.

The Data Protection Officer will want to take steps to contain the potential breach. They will want to recover the information and they will need to inform their Chair of Governors.

If a pupil is potentially in danger from the breach, their safety is a priority and they must be protected. Follow safeguarding procedures. Once they are safe, then an investigation can commence.

What are the criteria for deciding whether a potential breach requires an investigation?

The decision to investigate formally will depend mainly on whether the information has been disclosed and is uncontained. Both of these will also indicate the possible effect it will have on the people whose data has been disclosed. The following are some of the criteria that indicate when a potential breach needs further investigation and cannot be considered contained by the service:

- Sensitive personal information is disclosed to anyone who does not work for the Federation or LA and does not have a need to know.
- Sensitive personal information of pupils or staff is lost or stolen.
- Sensitive personal information, such as case review documentation, is emailed to several people who do work for the LA but who do not have a need to know.

Investigating the Potential Data Breach

Responsible Officer: Data Protection Officer / Executive Headteacher / Chair of Governors

When a potential breach meets the criteria for further investigation, the Federation needs to investigate the loss and produce a short report. In general, the report needs to answer four interrelated questions.

- What caused or allowed the breach to occur?
- Do the people affected by the breach need to be informed?
- Does the ICO need to be notified?
- What are the lessons to be learned to avoid a similar breach in the future?

Worked example

The Federation secretary reports that a child's assessment from the Educational Psychologist went to the wrong address. The person at the wrong address opened the assessment and read it. They contacted the Federation. This is a potential breach that needs to be investigated. It cannot be contained because the letter has been opened. If the letter had been collected before it had been opened, then it could be considered to have been contained. This needs further investigation, and may need to be referred to the ICO. The safety of the child should also be considered and additional safeguarding procedures may need to be followed.

A template for investigating data breaches is attached at the end of the document.

Beyond the containment and recovery phase, the investigation may reveal that the people affected by the breach need to be informed. When the Federation decides to notify the affected persons, it should have a clear purpose, for example, to enable individuals who may have been affected to take steps to protect themselves. If there is a safeguarding concern identified, the Federation should immediately follow its safeguarding procedures, for example, if the identity of a looked after child (LAC) at risk has been disclosed, this could affect the safety of the child and measures will need to be taken to protect the safety of the family. In extreme cases, for instance if a member of staff has lost or published personal data affecting children, it may be necessary to instigate disciplinary measures against the member of staff and consider referral to the LADO for further advice.

Please note: This decision is to tell the data subject so that they can take any steps they feel necessary to protect their personal information, such as from identity theft. This is not the formal notification of the ICO which is covered in the fourth decision stage following a formal data breach.

At the end of the investigation, the Federation may want to contact the data subject(s) and explain what went wrong and what has been done to fix it. A copy of the full data breach investigation report is not normally sent.

The investigation report will suggest whether the incident needs to be logged as a formal data breach.

Managing the Potential Breach

Responsible Officer: Data Protection Officer

Once a potential data breach report is completed the **third decision point** is reached. The decision now is whether the potential breach is to be logged as a formal data breach. **What are the criteria for recommending a formal data breach?**

The primary consideration will be the wellbeing of the people affected by the breach.

The following questions will help with making that decision.

- What type of data is involved?
- How sensitive is it? Is it sensitive because of its very personal nature (health records) or because of what might happen if it is misused (bank account details)?
- What has happened to the data? If data has been stolen, could it be used to harm the individuals it relates to?
- What does the data tell a third party about the individual? Is it only one detail about them, such as a telephone number, or does it include other details that could help a fraudster build a detailed picture?
- How many people are affected?
- Who are the people affected? For example, are they staff, customers, clients, suppliers, or vulnerable children and adults?
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

The severity of any potential breach needs to be considered in terms of the sensitivity of the information and the number of people involved. The matrix [Table 1] shows when a potential breach becomes an actual breach requiring further formal assessment. *The table is for guidance only and other circumstances may have to be considered.*

The Federation should use Table 1, below, when considering whether to recommend if a potential data breach investigation should result in the recording of a formal data breach.

Table 1

Number of People involved	**1000+**					
	100					
	50					
	5					
	1					
		e.g. Name, address	e.g. National Insurance number	e.g. Bank details, medical information	e.g. Details of a vulnerable child.	e.g. Full medical files or criminal file
	Sensitivity of the Information					
Key	**Unlikely to require recommending as a formal breach**		**Consideration should be given to recommending as a formal breach**		**Likely to require recommending as a formal breach**	

The table is only a guide. **The risk of harm to the individuals involved should be considered as the determining factor.**

Worked example

Here is a worked example to understand the difference between a near miss, a potential breach and a formal data breach. The formal data breach requires recording on the formal data breach log. All breaches start as potential breaches and then are recorded as near miss, potential breach, or formal breach.

Near Miss

Some data security breaches will not lead to risks beyond inconvenience to those who need the data to do their job. For example, a damaged laptop where the files are backed up and can be recovered, has a lower level of risk and can be recovered and managed by the Federation. This has to be investigated as potential breach. As the information can be recovered or reconstructed and the information is not in the public domain, then the data subjects would not have suffered damage or distress. It would be logged as a **near miss.** An apology would not need to be sent.

Potential data breach

If the data cannot be recovered and it will have an effect on the data subject because the Federation has to reconstruct the data set. Even though the data is not in the public domain, it would be investigated and logged as a potential breach. The investigation should reveal why the data was stored in such a way it could become corrupted and was not recoverable. If the data subject was not affected directly by the breach, then they would not need to be informed. If they were affected, such as a missed appointment as a result, then they would need an apology.

Formal data breach

A spreadsheet with the medical assessments including psychological assessments of vulnerable children was emailed to 400 taxi firms. The breach cannot be contained. It involves sensitive information of more than 5 people. This would require an investigation.

The investigation should recommend it be logged as a formal data breach based on the amount of information, that it was in the public domain, the sensitivity of the information and the potential harm to the children. The harm to the individuals would be greater because their information was in the public domain. An apology would need to be issued. This would need to be logged as a formal breach and the Federation would need to consider whether it will inform the ICO.

Final Evaluation and Response

Responsible Officer: Executive Headteacher / Data Protection Officer / Chair of Governors

The final evaluation process is done by the Head, DPO and Governing Body to consider the causes of the breach and the lessons that need to be learned. The investigation report indicates how effective the Federation was in response to the breach. The Federation should also seek advice from the School and Governor Support Service.

The Federation should implement any actions highlighted by the report**.**

Formal Notification of Breaches

Responsible Officer: Executive Headteacher / Data Protection Officer / Chair of Governors

The **fourth decision stage** is whether the data breach was severe enough to require the Federation to inform the Information Commissioner's Office. The decision to notify the ICO will be made by the Federation with additional advice from the School and Governor Support Service.

Please note that this decision stage is different from notifying a data subject of the data breach.

Data Breach Investigation Report Template

Root Cause Analysis (RCA) - Investigation Report Template – Guidance.

Write your investigation report in the right-hand column (column B)

To help in writing the report, refer to summary guidance in column A.

Additional help can be found in the 'Guide to RCA investigation report writing'.

If, when you are carrying out your investigation, there is no information against a heading, please explain why this is the case. (For example, if you do not know the date of an incident, but only the date it was reported, then leave the incident date blank and explain the date is not known.)

If issues arise which require a new heading this can be added as a new row.

Once you have completed column B, you need to delete column A. * <u>All that is required is column B</u>*

First, delete all guidance both here and in the template below.

A copy of this report will need to be retained in the Federation and may be needed by other agencies (Police, ICO, Legal Team) in assisting the Federation in dealing with the consequences of the breach.

Column A	Column B
Quick reference guide	**Type your investigation report in this column**
Incident Date	
Incident Number	Add your number
Author(s) / Investigating Officer	Name of person
Report Date	Date
Incident description and consequences (Concise incident description, including number of data subjects.)	The personal information of 25 vulnerable children were disclosed when an email was sent to external transport list rather than an internal transport list.
Information Recovered	Yes or No.
Decision as to whether those individuals whose data has been breached and are to be notified.	*Example only (please delete and add your own findings)* The 25 people included bank details. The individuals concerned have been notified to allow them to be vigilant for any suspicious activity on their account.
Chronology of events (For complex cases any summary timeline included in the report should be a summary.)	The key points of the event: when discovered, when last use of data, when authority notified, when information recovered if recovered, when data subject informed of risk etc.
Contributory factors (A list of significant contributory facts.)	Over the years email addresses had been added, causing the team to lose track of the internal and external lists.
Root Causes (These are the most fundamental underlying factors contributing to the incident that can be addressed. Root causes should be meaningful (not sound bites such as communication failure) and there be a clear link, by analysis, between root CAUSE and EFFECT.)	Staff involved have not had training on use of internal and external lists. Internal and external lists have names that are only different by one letter. There is no procedure for creating distributions lists to be used by service.

Lessons learned (Key issues identified which may not have contributed to this incident but from which others can learn.)	The external lists should be marked clearly and consistently as external.
Type of breach	Please tick one of the following: Near miss ☐ Potential breach ☐ Further action: ☐ *please provide details* No further actions ☐ Formal breach ☐
Recommendations (Numbered and referenced) Recommendations should be directly linked to root causes and lessons learned. They should be clear but not detailed. (Detail belongs in the action plan.) It is generally agreed that key recommendations should be kept to a minimum wherever possible. All recommendations are to be Specific, Measurable, Achievable, Realistic and Timely. – SMART.	Ensure all email lists are reviewed so that external lists are clearly marked. All staff are instructed about the use of external email lists.
Arrangements for shared learning (Describe how learning has been or will be shared with staff and other organisations.)	*Example only (please delete and add your own findings)* • Share findings with other Federations sharing similar activities. • Share findings to identify opportunities for sharing outside the organisation.
Outcome (The conclusion of the investigation should state whether the author believes the breach should be logged formally or not.)	*Example only (please delete and add your own findings)* As the breach resulted in sensitive personal information being inappropriately shared with more than 10 people, it is recommended that this be recorded as a formal data breach.
Executive Headteacher, Data Protection Officer and Chair of Governors **Date**	