UK General Data Protection Regulation (UK GDPR) Personal Data Breach Procedure

Blessed Edward Bamber Catholic Multi Academy Trust

VERSION: 2.0

ADOPTED: AUTUMN TERM 25

NEXT REVISION: AUTUMN TERM 27

Blessed Edward Bamber
Catholic Multi Academy Trust

Corinthians 4:2

Now it is required that those who have been given a trust must prove faithful.

Version Control

Date of last review	AUTUMN TERM 2025
Date of next review	AUTUMN TERM 2027
Review period	2 YEARS
Policy Status	TRUST WIDE
Owner	CFO
Approver	CEO/FSP
Version	2.0

Previous versions

Version	Author	Date	Changes
1.0		Spring 25	
2.0		Autumn 25	Incident report updated, contact information for DPO updated

This is a Trust-Wide Policy which applies to all academies within the Trust

Contents

1. Introduction

The UK General Data Protection Regulation (UK GDPR) places a requirement on Schools / Academy Trusts to have a formal process in place to manage personal data breaches.

This procedural guide describes what a personal data breach is and the process which must be followed in the event of a breach.

This guidance applies to all employees, partners, volunteers, suppliers, contractors and Governors (collectively referred to as 'users') who process, have access to, hold or who are responsible for the School/Academy's personal data. All users must understand and adhere to this guidance, with it applying to all personal data, regardless of whether it is held in a paper or electronic format.

2. Personal Data Breach Definitions

A personal 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. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- Access to personal data by an unauthorised third party e.g. a cyber-attack;
- Sending personal data to an incorrect recipient e.g. email or a letter;
- Paper records containing personal data being lost or stolen;
- Electronic devices containing personal data being lost or stolen; • Alteration of personal data without permission; and
- Loss of availability of personal data.

See Appendix 1 for real life examples.

A personal data breach is 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 without permission;
- If someone accesses the data or passes it on without proper authorisation;
- If the data is made unavailable, for example, when it has been encrypted by ransomware, or lost or destroyed.

When a security incident takes place, the School/Academy should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.

3. Personal Data Breach Process

Should a user discover a data breach, they must **immediately** report this to their respective School Data Protection Lead.

Your School/Academy Data Protection Lead is:
Insert name
Insert postal address.
And / or email **insert email address.**

If the Data Protection Lead is unavailable it should be brought to the attention of an alternative member of the Senior Leadership Team (SLT).

The Data Protection Lead or member of SLT should immediately report the personal data breach to the School/Academy's Data Protection Officer (DPO) using the Data Breach Notification Form in Appendix 2

The DPO will then initiate an investigation of the personal data breach and advise the School/Academy on any actions it should take to contain or recover the personal data. The DPO will conduct an assessment of the likelihood and severity of the resulting risk to the data subject's rights and freedoms. Based on this assessment the DPO will issue formal guidance to the School/Academy on whether the ICO or data subject should be notified. The DPO will work closely with the School/Academy with regards to any remedial actions to prevent a reoccurrence.

The contact details for the Trust's designated DPO are as follows:

Data Protection Officer, Shard Business Services
dpo@shardbusinessservices.co.uk

4. ICO Notification – Criteria

When a personal data breach has occurred, the DPO will undertake an assessment of the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then the DPO will advise the School/Academy that the incident is required to be referred to the ICO. However, please note that the specific ICO Breach Notification Form must only be completed and submitted by the DPO.

If it is unlikely to result in a risk to people's rights and freedoms then the School/Academy does not have to notify the ICO. However, once it is decided that the breach does not need to be reported, the decision must be justified and the reasons for that decision must be documented by the DPO.

In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals.

Recital 85 of the UK GDPR explains that:

> *'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'.*

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job.

If a data processor contracted on behalf of the School/Academy has encountered a personal data breach, then under Article 33(2) of the UK GDPR, the data processor must inform the School/Academy without undue delay and as soon as the data processor becomes aware.

The requirements on breach reporting should always be detailed in the contract between the School/Academy and its processor. This requirement then allows School/Academy to take steps to address the breach and meet its breach-reporting obligations.

5. ICO Notification – Timeframes

The DPO must report a notifiable breach to the ICO without undue delay**,** but not later than **72 hours** after becoming aware of it. If School/Academy takes longer than this, then it must give reasons to the ICO for the delay.

The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. Article 33(4) allows the organisation to provide the required information in phases, as long as this is done without undue further delay.

6. ICO Notification – Consent

When the DPO reports a breach to the ICO, the UK GDPR states they must provide:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- 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; and
- 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.

Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of your global turnover. The fine can also be combined with the ICO's other corrective powers under Article 58 of the UK GDPR**.**

7. Data Subject Notification

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says the School/Academy must inform those concerned directly and without undue delay. When a personal data breach has occurred, the DPO will conduct an assessment of the likelihood and severity of the resulting risk to people's rights and freedoms, and advise the School/Academy whether they are required to notify the data subject.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, the DPO will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, users will need to 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 effects of a breach.

If the School/Academy decide not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The School/Academy should also remember that the ICO has the power to compel them to inform affected individuals if they consider there is a high risk. In any event, the DPO should document their decision-making process in line with the requirements of the accountability principle.

8. Data Breach Repercussions

8.1 ICO

The ICO has the power to take action against organisations in line with Part 5 of the Network and Information Systems Regulations 2018. The regulations are primarily aimed at improving cybersecurity and relates to any 'incident' that has an impact on a service which includes 'noncyber' causes.

The ICO have the following enforcement powers:

- **Information notices**
  Under Regulation 15(3), the ICO may serve an 'information notice' (IN)
  The IN will describe the information the ICO require, the reasons why it is required, how it should be provided and the time period.
- **Enforcement notices**
  Under Regulation 17(2), the ICO may serve an enforcement notice (EN) when they have reasonable grounds to believe an organisation have failed to:
  - fulfil their security obligations o notify the ICO of a security incident o comply with their notification obligations o notify the public about any incident, if it was deemed a requirement to do so o comply with an Information Notice o complying with inspection requirements
- **Inspection powers**
  Under Regulation 16(2), the ICO has the power to conduct an inspection to see if an organisation has fulfilled their security obligations
- **Penalty notices**
  Regulation 18(2) gives the ICO the power to serve a penalty notice on an organisation in certain circumstances. Penalties will be issues that are appropriate and proportionate to the failure.

8.2 Right to Compensation

Under Article 82 of the UK GDPR '*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered*'

- Material damage = financial loss.
- Non-material damage = the individual has suffered distress.

8.3 Employee

All members of staff have responsibility for how the School/Academy collects, holds and processes personal data. Staff found to be in breach of the Personal Data Breach Procedure, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Breaches of any School/Academy policies and procedures will be dealt with as a matter of conduct, capability or performance via the School/Academy's existing Human Resources policies and procedures.

8.4 Criminal Proceedings

Section 170 of the Data Protection Act 2018 states that it is a criminal offence for a person to knowingly or recklessly obtain, disclose or procure personal data without the consent of the data controller.

Examples include:

- School data being taken, retained or transferred unlawfully
- Deliberately deleting School data to prevent it being disclosed in response to a Subject Access Request (SAR)
- Re-exposing previously redacted material

The School/Academy, as a data controller has a legal responsibility to report potential offences to the ICO where an assessment will be carried out by their Criminal Investigation Team. During their assessment, they will decide where there is sufficient evidence to support a prosecution or if it is in the public interest to prosecute.

9. Review

The Trust will review this procedure regularly to ensure continued compliance with data protection regulations. For any further questions regarding this procedure, contact the trust DPO at dpo@shardbusinessservices.co.uk

Appendices to Data Breach Procedure

Appendix 1 – Real life examples of breaches

Corringham school apologises after sharing personal pupil data 14 December 2023  The email contained information about pupils aged between Year 7 and Year 11	• A school has apologised for sending an email to parents which listed the personal data of 69 pupils who were being disciplined for bad behaviour. • The message included an attachment which contained information about free school meal eligibility and pupils' special educational needs (SEN) status. • Made a self referral to the Information Commissioner's Office (ICO).
Schools hit by cyber attack and documents leaked 6 January 2023  Following a hack, Vice Society makes demands for money to prevent it leaking documents on the dark web	• Highly confidential documents from 14 schools have been leaked online by hackers. Vice Society makes demands for money to prevent it leaking documents on the dark web • Hacking' is a process where by a 'hacker' gains unauthorised access to a system, network or computer by exploitation of its areas of weakness. • Folders accessed consisted of passport scans for pupils and parents, contractual offers, teaching documents and student bursary fund recipients.
	• The former head teacher of a school in Ashford was ordered to pay more than £1,000 after he admitted unlawfully obtaining school children's personal data.

Ex-Meadhurst School head fined for unlawfully transferring pupil data

He had "no valid explanation" for how pupil data from Spelthorne and The Russell schools ended up on the server at his new school

By Christopher McKeon Senior Reporter

Bookmark

Comments

Enter your postcode for local news and info

Enter your postcode

Go

In Your Area

Darren Harrison, former headteacher of Spelthorne School, was fined for breaches of the Data Protection Act involving unlawful processing of pupils' information (Image: Surrey Advertiser)

- The staff member was suspended for six months
- The staff member had no lawful reason to process the data and provided "no valid explanation" for how it had appeared on the server, instead claiming they had deleted the personal data from his USB stick.
- The former Headteacher appeared at Ealing Magistrates' Court and admitted two offences of unlawfully obtaining personal data and was subsequently fined.

Appendix 2 – Data Breach Reporting form

Use this Form to report a potential data breach to the School's Data Protection Officer (DPO). A form should be submitted immediately when you become aware of a potential data breach because the school must report a notifiable breach to the ICO without undue delay, but not later than **72 hours**. If this form is being submitted later please explain why.

1. Name of School:	
2. Name of employee reporting the potential data breach:	
3. Job title of employee reporting the potential data breach:	
4. Name of employee responsible for the potential data breach:	

5. What date was the incident discovered?	6. What time was the incident discovered?	7. Date the Incident Occurred	8. What time did the incident occur?

9. Police and Crime log number (if applicable)

10. Describe the incident *(include type of data, format of data e.g. electronic or physical)*

11. How did the incident occur? (*E.g. human error, phishing attack)*

12. What steps have been taken to contain/recover personal data? What steps have been taken to migitate/minimise the effect of the breach on affected data subjects? Haae any preventative measures been taken prior to reporting?

13. Approximately how many people have been affected?

14. Who has been affected?	Please mark
Pupils (including former pupils)	☐
Parents / Carers / Guardians	☐
Employees	☐
Governors / Trustees	☐
Other (Please specify below)	☐
Other:	

15. What category of personal data has been placed at risk?	Please mark
Basic personal identifiers e.g. name and contact details	☐
Criminal convictions or offences	☐
Data revealing racial or ethnic origin	☐
Economic and financial data, e.g. credit card numbers, bank details	☐
Gender reassignment data	☐
Genetic or biometric data	☐
Health data	☐
Identification data e.g. usernames, passwords	☐
Official documents e.g. driving licence	☐

Political opinions	☐
Religious or philosophical beliefs	☐
Sex life data	☐
Sexual orientation data	☐
Trade union membership	☐
Other (Please specify below)	☐
Other:	

16. Have you informed the data subjects that this incident occurred?	Yes	No	Not Applicable
Please mark	☐	☐	☐

17. Please provide an estimate regarding the likelihood of harm caused following this data breach	Please mark
Not Occurred	☐
Not Likely	☐
Likely	☐
Highly Likely	☐
Occurred	☐

18. Please provide an estimate regarding the impact caused following this data breach (actual and considered potential impact)	Please mark
Effect	☐
Minor	☐
Adverse	☐
Serious	☐
Catastrophic	☐

19. Has the staff member responsible for the breach completed data protection training in the last two years? If so, what type of training?

20. Was the breach caused by a cyber incident? If yes, has system integrity been affected, and how? What is the potential impact? Please provide as much information as possible.

21. Is there any further information you would like to provide?

The contact details for the School/Academy designated DPO are as follows:

Data Protection Officer, Shard Business Services

Email Address: dpo@shardbusinessservices.co.uk
Telephone Number: 07516068886