Budmouth Academy

DATA BREACH POLICY

Version control	
Data Breach Policy [2022-09-01]	Reviewed and updated to reflect reference to UK GDPR and the cyber security policy.
Data Breach Policy [2021-04-01]	Reviewed and updated previous version to align with new DPO appointment.

Date of next review:	**September 2024**	**Owner:**	**Director of HR & Compliance**
Type of policy:	**Trust Template**	**Approving Body:**	**Executive Operational Board**

DATA BREACH POLICY

1. Introduction

Budmouth Academy is committed to good practice with regards to data protection. This policy, based on the Aspirations Academies Trust template Data Breach Policy, is aimed at ensuring the application of good practice at the Academy.

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and the Academy's procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the Academy of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Academy's Disciplinary Policy up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the Academy and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

2. Definitions

2.1 Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Academy possesses or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

2.2 Special category data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2.3 Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

2.4 Data subject

Person to whom the personal data relates.

2.5 ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

3. Responsibility

The Director of Business and Support Services carries the responsibility of designated lead officer for data protection at the Academy and has overall responsibility for breach notification within the Academy. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches. For ease of reference through the remainder of this document they are referred to as *the* ***Academy DP Lead***.

In the absence of the Academy DP Lead, alternative contacts within the Academy are the main office or the Principal. In the absence of any appropriate contact at the Academy, the Aspirations Director of HR and Compliance or Deputy Director of HR and Compliance may be contacted (they act as the *Trust DP Lead*).

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

While normally the *Academy DP Lead* or *Trust DP Lead* would be contacted in the first place, questions about the operation of this policy or the UK GDPR may be raised with the DPO. Any concerns that this policy is not being or has not been followed may also be raised with the DPO.

The DPO's contact details are set out below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

4. Security and data related policies

Staff should refer to the following policies that are related to this policy:

- **Information Security Policy.** This sets out the Academy's guidelines and processes on keeping personal data secure against loss and misuse.

- **Data Protection Policy.** This sets out the Academy's obligations under UK GDPR about how personal data will be processed.

- **Cyber Security Policy**. This sets out the Academy's obligations and guidelines for cyber security issues.

These policies are also designed to protect personal data and can be obtained from the Academy DP lead.

5. Data Breach Procedure

5.1 What Is a personal data breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (this list is not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

5.2 When does it need to be reported?

The Academy must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be

more than just losing personal data. The breach must be of a nature that, if unaddressed, it is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a *high risk* to the rights and freedoms of individuals then the individuals must also be notified directly.

6. Reporting a data breach

Where someone knows or suspects a personal data breach has occurred or may occur which meets the criteria above, they should: -

- Complete a data breach report form (which can be obtained from *the Academy DP Lead- APPENDIX 01*
- Email the completed form to *the Academy DP Lead*.

Where appropriate, they should liaise with their line manager about completion of the data breach report form. Breach reporting is encouraged throughout the Academy and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, *the Academy DP Lead* or the DPO.

Once reported, the reporting person should not take any further action in relation to the breach. In particular they must not notify any affected individuals or regulators or investigate further. *The Academy DP Lead* will acknowledge receipt of the data breach report form and take appropriate steps as set out below.

7. Managing and recording the breach

On being notified of a suspected personal data breach, *the Academy DP Lead* will notify the DPO and *the Trust DP Lead*. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to: -

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the Academy's data breach register;
- Notify the ICO where required;

- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

8. Notifying the ICO

The *Academy DP Lead* will decide, in consultation with the DPO, how notification to the ICO will be progressed when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of weekends and school holiday periods (i.e. it is not 72 working hours). If the Academy is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

9. Notifying data subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the *Academy DP Lead* will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the Academy has taken or intends to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the *Academy DP Lead* will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the Academy will consider alternative means to make those affected aware (for example by making a statement on the Academy website).

10. Notifying other authorities

The *Academy DP Lead* in consultation with the *Trust DP Lead*, the Principal and the DPO will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

11. Assessing the breach

Once initial reporting procedures have been carried out, the Academy will carry out all necessary investigations into the breach. The investigation will be carried out by the Academy DP Lead or an investigation officer to whom they delegate this task.

The investigation officer will identify how the breach occurred and in conjunction with the Academy DP Lead, take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. They will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the Academy will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the Academy; and
- Any other wider consequences which may be applicable.

12. Preventing future breaches

Once the data breach has been dealt with, the *Academy DP Lead* in conjunction with the Principal and any other relevant staff of the Trust, will consider the Academy's security processes with the aim of preventing further breaches. This will involve:

- Establishing what security measures were in place when the breach occurred;
- Assessing whether technical or organisational measures can be implemented to prevent the breach happening again;
- Considering whether there is adequate staff awareness of security issues and looking to fill any gaps through training or tailored advice;
- Considering whether it is necessary to conduct a privacy or data protection impact assessment;
- Considering whether further audits or data protection steps need to be taken;
- Updating the data breach register;

- Debriefing as appropriate senior management, local governors and trustees following the investigation.

13. Reporting data protection concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and the Academy encourages any concerns to be reported to the *Academy DP Lead* or the DPO (even if they do not meet the criteria of a data breach). This can help capture risks as they emerge, protect the Academy from data breaches and keep its processes up to date and effective.

14. Training

The Academy will ensure that staff are trained and aware of the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them.

15. Monitoring

The *Academy DP Lead* in conjunction with the Principal and Trust DP Lead will monitor the effectiveness of this and related policies and procedures. A full review and update as appropriate will be undertaken at least every two years.

Any monitoring and review will include looking at how policies and procedures are working in practice to reduce the risks posed to the Academy.

APPENDIX 1 – Data Breach Form

Please provide details below of the personal data breach that has or may occur and email the completed form to *the Academy DP Lead*.

DATA BREACH REPORTING FORM	
Your name/position	
Date of breach	
Summary information of the breach (where known this should include details of): **1) how the breach occurred** **2) the data affected** **3) the individuals affected** **4) any other consequences** **Please use separate sheet if further space required.**	
Signed	**Date**
Once completed please submit to Academy DP Lead.	