The 3-18 Education Trust

Data Breach Procedure

Every individual is in a great school.

Approved: Autumn Term 2023

www.318education.co.uk

Contents

Introduction 3
Definitions 3
Personal Data 3
Special Category Data 3
Personal Data Breach 3
Data Subject 4
Information Commissioner's Office 4
Responsibility 4
Security and Data Related Policies 4
Data Breach Procedure 4
What is a personal data breach? 4
When does it need to be reported? 5
Reporting a Data Breach 5
Managing and Recording the Breach 5
Notifying the ICO 6
Notifying Data Subjects 6
Notifying Other Authorities 6
Assessing the Breach 6
Preventing Future Breaches 7
Reporting Data Protection Concerns 7
Training 7
Links to other Policies and Procedures 8
Procedure Monitoring and Review 8
Monitoring 8
Review 8
Appendix A – Data Breach Reporting Form 9

Introduction

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 The 3-18 Education Trust (Trust) to report actual or suspected data breaches and the procedure for dealing with breaches is set out below. All members of staff, volunteers, trustees and local governors (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 Trust 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 procedure may be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

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

Definitions

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 we possess 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 example, 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.

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.

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.

Data Subject
An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

Information Commissioner's Office
The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. ICO is an executive non-departmental public body, sponsored by the Department for Science, Innovation and Technology.

Responsibility

The IT Director has overall responsibility for breach notification within the Trust. 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.

In the absence of IT Director, please contact the School's Business Manager.

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

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

Security and Data Related Policies

Staff should refer to the following policies that are related to this Data Breach Procedure:

- Information Security Policy and Procedure which sets out the Trust's guidelines and processes on keeping personal data secure against loss and misuse.
- Data Protection Policy which sets out the Trust's obligations under UK GDPR about how they process personal data.
- Online Safety Policy which sets out the Trust's obligations and guidelines for acceptable online use and cyber security issues.

These policies are also designed to protect personal data.

Data Breach Procedure

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 (but are 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.

When does it need to be reported?
The Trust 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 and if unaddressed, the breach 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.

Reporting a Data Breach
If staff know or suspect a personal data breach has occurred or may occur they should complete a data breach report form which can be obtained from the School's Business Manager or Appendix A. Email the completed form to the School's Business Manager, IT Manager or IT Director.

Where appropriate, staff should liaise with their line manager, or appropriate, about completion of the data report form. Breach reporting is encouraged throughout the Trust 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, School's Business Manager, IT Manager or IT Director.

Once reported, no further action in relation to the breach must be taken by staff. In particular staff must not notify any affected individuals or regulators or investigate further. The School's Business Manager, IT Manager or IT Director will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach
On being notified of a suspected personal data breach, the School's Business Manager, IT Manager or IT Director will notify the DPO. 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 Trust'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.

Notifying the ICO
The DPO will notify the ICO 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 school holidays (i.e., it is not 72 working hours). If the Trust are 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.

Notifying Data Subjects
Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the School's Business Manager, IT Manager or IT Director will determine whether it is necessary to notify individuals directly of the breach, The School's Business Manager IT Manager or IT Director will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

Where agreed the School Business Manager, IT Manager or IT Director will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the Trust have (or intended) to take to address the breach.

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 Trust will consider alternative means to make those affected aware (for example, by making a statement on the School website).

Notifying Other Authorities
The Trust 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/ies.
- The Police (for example, if the breach involved theft of equipment or data).

This list is non-exhaustive.

Assessing the Breach
Once initial reporting procedures have been carried out, the Trust will carry out all necessary investigations into the breach.

The Trust will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. Ways to recover, correct or delete data (for example, notifying insurers or the Police if the breach involves stolen hardware or data) will be identified.

Having dealt with containing the breach, the Trust 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 Trust and School.
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the Trust will consider its security processes with the aim of preventing further breaches. This will include the following actions:

- Establish what security measures were in place when the breach occurred.
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again.
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice.
- Consider whether it is necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken.
- To update the data breach register.
- To debrief the trust Board, Local Governing Bodies, schools' management following the investigation.

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 Trust encourages Staff to report any concerns (even if they do not meet the criteria of a data breach) that they may have to the IT Director, School's Business Manager or the DPO. This can help capture risks as they emerge, protect the Trust from data breaches and keep processes up to date and effective.

Training

The Trust will ensure that Staff are trained and aware on the need to report data breaches, how to detect data breaches and the procedures of reporting data breaches.

This procedure will be shared with staff.

Links to other Policies and Procedures

Data Protection Policy and Subject Access Request Procedure
Information Security Policy and Procedure
Operation of CCTV Procedure
Protection of Pupils Biometric Information and Consent to use Biometric Data
Records Management Policy and Retention Schedule.

Procedure Monitoring and Review

Monitoring

The Chief Executive Officer, in conjunction with the IT Director and DPO, will monitor the outcomes and impact of this procedure on an annual basis.

Review

Member of Staff Responsible	Chief Executive Officer
Relevant Guidance/Advice/Legal Reference	The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 Data Protection Act 2018 (DPA 2018) Protection of Freedoms Act 2012. ICO Guidance on Personal Data Breaches
Policy Adopted By	Trust Board
Date of Procedure	Autumn Term 2023
Review Period	Annually
Date of Next Review	Autumn Term 2024

Appendix A – Data Breach Reporting Form

Name of person completing this form	
Name of person discovering data breach (if different)	
School	
Position in School	
About the Data Breach	
Please described what happened.	
Please describe how the incident occurred.	
How did you discover the beach?	
To the best of your knowledge, was the breach caused by a cyber incident? (Yes, No, Don't Know)	
To the best of your knowledge, when did the breach happen? (Date and Time)	
To the best of your knowledge, when did you discover the breach happen? (Date and Time)	
To the best of your knowledge, describe any detriment to individuals that has arisen so far,	