Zest Academy Trust

Data Breach Policy

Approved & Adopted by Trust Board: 19 June 2018
Review Period: Biennial
Policy Date Last Reviewed/Approved: 07/10/2020
Person Responsible: COO
Version Number: 2

Zest Academy Trust, Waterloo Road, Blackpool, FY4 3AG
T 01253 315370 E admin@zestacademytrust.co.uk W www.zestacademytrust.co.uk

CEO Mark Hamblett

Introduction

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

The GDPR places obligations on employees, Trustees and Academy Council Members to report actual or suspected data breaches to the Data Protection Officer (DPO). All employees are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Training is also provided to employees to enable them to carry out their obligations within this policy.

Employees who breach this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust disciplinary policy up to and including summary dismissal depending on the seriousness of the breach.

Definitions

Data subject
An individual about whom such personal data relates to.

Personal data
Personal data is information relating to an individual where they can be identified directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
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 an individual.

Special category data
Special categories of personal data refer to an individual data subject's, race, ethnic origin, political view, religion, trade union membership, genetics, biometrics, health, sex life or sexuality.

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

Responsibility

The overall responsibility for breach notification is Nicola Lea. 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 Nicola Lea, please contact Mark Hamblett.

Data Protection Named Contact for the Trust

Mrs Nicola Lea COO (Chief Operations Officer)
Nicola.Lea@zestacademytrust.co.uk

Data Protection advisors
DPOservice@schoolspeople.co.uk

Reporting and recording a data breach

Data breaches or near misses may be identified as part of everyday business and may be identified by the office at the first point of contact, by a parent or pupil or by a third party.

What is a data breach?
Personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. Examples of data breaches are:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- "Blagging" offence where information is obtained by deceiving the organisation who holds it

Human error is the most common cause of data breach and may include:

- Theft of loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal / sensitive recipient

Reporting a breach
If you suspect or know a personal data breach has occurred then you must:

- Complete an online data report breach form, which accessible by the Trust portal

This notification will automatically be referred to Nicola Lea for investigation. Data breach reporting is encouraged through the Trust and employees should seek advice if they are unsure whether a breach should be reported.

The Trust also encourage near misses to be reported via the data breach form, so that the Trust can identify areas for improvement within the organisation and make improvements.

Once reported you should take no further action in relation to the breach.

Notifying others
If the data breach is likely to result in the rights and freedoms of individuals being put at risk and have a significant detrimental effect of them then the Independent Commissions Office (ICO) need informing.

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 of physical safety or reputation
- Exposure to identity theft
- Exposure to the private aspect of an individual's life becoming known to others

The ICO should be notified without undue delay and where possible within 72 hours of being aware of the data breach. If the Trust are unsure of whether the breach should be reported or not the assumption will be to self-report.

If the breach is identified as high risk then the individual(s) whose rights and freedoms have been affected will without undue be notified of the data breach.

On occasions the Trust may need to consider if other third parties need to be notified of the data breach. These may include, parents, local authority, insurers and police.

Assessing the data breach

Upon receiving the initial data breach notification, the Trust will notify Nicola Lea who will decide how best to deal with the case. In the majority of instances, a formal investigation will be required to establish the scope of the breach.

Containing the breach
The Trust will initially look to contain or stop the breach in order to minimise further loss, destruction or unauthorised disclosure of personal data. These steps might include:

- Attempting to recover any lost equipment or personal data
- Shutting down any IT systems

- Contacting the business office team and others so they are prepared for any potential inappropriate enquires about the affected data subjects
- If an inappropriate enquiry is received staff should attempt to obtain the enquirers name and contact details and confirm that they will ring the enquirer back
- If bank details have been lost or stolen contact banks directly for advice on preventing fraud
- If the breach includes any entry codes or passwords then those codes must be changed immediately and the relevant organisations and employees informed

Investigating the breach
Having dealt with containing the breach, the Trust will consider the risks associated with the breach. These factors will determine whether further steps need to be taken, for example notifying the ICO. These factors include:

- The type of information and how sensitive it is
- The number data subjects are affected by the breach
- The type of protection in place, i.e. encryption
- What has happened to the data
- Whether the information could be put to any illegal or inappropriate uses
- Who and how many data subjects have been affected
- What could the data tell a third party about the data subject
- What are the likely consequences of the data breach on the Trust
- Any other wider consequences which may be applicable

The initial investigation should be completed as a matter of priority and where possible within 24 hours of the breach being discovered. A further review of the causes of the breach and recommendations on prevent future breaches will also be undertaken.

Preventing further breaches
Once the data breach has been dealt with the Trust will review its security processes and procedures with the aim of preventing further security breaches. In order to do so the following will be considered:

- Were the Trusts security measures adequate at the time of the breach
- Consider whether there was adequate staff awareness
- Consider whether a data protection impact assessment is necessary
- Consider if further data protection audits are necessary
- Update Trustees / Academy Council Members of the brief following the investigation

Monitoring

The Trust will monitor the effectiveness of all policies and procedures.

Related policies
The following policies are related to this data protection policy:

- data retention policy
- data protection policy
- working at home policy
- remote working policy
- disclosure and barring service storage policy
- privacy notices

These policies are also designed to protect personal data and can be found at www.zestacademytrust.co.uk