GREENSHAW
LEARNING TRUST

GLT Data Breach Procedure

ALWAYS
LEARNING

Greenshaw Learning Trust
Data Breach Procedure

Contents

PART A 3
1.1. Application 3
1.2. Approval and review 3
1.3. Terminology 3
1.4. Responsibilities 4
1.5. Associated policies and procedures 4
PART B 5
2. What is a Data Breach? 5
3. Dealing with a Data Breach 5
4. Assessing The Breach 6
5. Preventing Future Breaches 7
Annex A – Judicium / ICO Data Breach Reporting Form 8

PART A

1.1. Application

This GLT Data Breach Procedure applies to the Greenshaw Learning Trust as a whole and to all the schools in the Trust and the Trust Shared Service, in accordance with and pursuant to the Communications Policy of the Greenshaw Learning Trust.

The Greenshaw Learning Trust, including all the schools, their Trustees, governors and staff, must abide by this GLT Data Protection Policy.

This Procedure is subject to the Trust's Scheme of Delegation for Governance Functions. If there is any ambiguity or conflict then the Scheme of Delegation and any specific alteration or restriction to the Scheme approved by the Board of Trustees takes precedence.

In implementing this Proceducre and associated policies and procedures the governing body, Headteacher and school staff, and Trust Shared Service staff, must take account of any advice or instruction given to them by the GLT Data Protection Officer, the GLT CEO or Board of Trustees.

If there is any question or doubt about the interpretation or implementation of this Policy, the GLT CEO should be consulted.

1.2. Approval and review

Maintenance of this Procedure is the responsibility of the GLT CEO.

This Procedure was approved by the Board of Trustees on: 23 July 2021.

This Procedure is due for review by: July 2024.

1.3. Terminology

The Trust means the Greenshaw Learning Trust (GLT).

- School means a school within the Greenshaw Learning Trust.
- Headteacher means the headteacher or principal of the school.
- CEO means the chief executive officer of the Greenshaw Learning Trust.
- Governors and Trustees includes governors, Trustees, non-governor members of Trust Committees and members of the Trust Panel.
- Governing body means the committee of the Board of Trustees to which Trustees have delegated appropriate powers and functions relating to the governance of the school.
- GLT Data Protection Officer means Judicium Consulting Ltd.
- School Data Protection Lead means the point of contact for data protection matters for members of staff, students and parents within the school
- Data Subject means an individual about whom such personal information is stored.
- Data Controller means the organisation storing and controlling information regarding data subjects which is Greenshaw Learning Trust.

In this policy references to the Greenshaw Learning Trust will be read as including the Trust Shared Service and all schools in the Greenshaw Learning Trust.

References in this Procedure to a school in the Trust should also be read as the Trust Shared Service for services, functions and members of staff of the Trust that are not contained within a school budget and/or are not the responsibility of a Headteacher and/or Governing Body. With respect to the Trust Shared Service, references in this Policy to the responsibilities of the Headteacher and Governing Body should be read as the GLT CEO and the Trust Shared Services Committee respectively.

1.4. Responsibilities

It is the responsibility of the governing body and Headteacher of each school, and the Board of Trustees and GLT CEO for the Trust Shared Service, to ensure that their school/service and its staff adhere to this GLT Data Protection Policy; in implementing this Policy the governing body, Headteacher and Trust staff must take account of any advice given to them by the GLT Data Protection Officer, GLT CEO and/or Board of Trustees.

For the purposes of data protection legislation the Greenshaw Learning Trust is the Data Controller, and can be contacted by writing to Greenshaw Learning Trust, Grennell Road, Sutton, SM1 3DY.

The GLT Data Protection Officer is: Judicium Consulting Limited.
Email: dataservices@judicium.com
Address: 72 Cannon Street, London, EC4N 6AE
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

Each Headteacher will appoint a School Data Protection Lead to be the point of contact for data protection matters for members of staff, students and parents of their school, and to liaise with the GLT Data Protection Officer. The name and contact details must be provided to the GLT Data Protection Officer and will be made available on the school website or by contacting the school.

1.5. Associated policies and procedures

- This GLT Data Breach procedure is a constituent part of the GLT Data Protection Policy

.

PART B

2. What is a Data Breach?

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.

A personal data breach can be 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; 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.

Examples of data breaches are:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data;
- leaving a PC unattended so a student or staff member can access data;
- inadvertently displaying data to a classroom on a screen;
- sending information about a child to the wrong address or email address;
- any breach of the data protection principles.

3. Dealing with a Data Breach

All members of staff in Greenshaw Learning Trust must be aware of what constitutes a data breach and what action to take in the event of a breach.

All breaches must be reported to the school / service Data Protecton Lead, in the first instance and as soon as discovered and reported to the GLT Data Protection Officer through the JEdu platform by following the instructions on the 'Breaches' link on the platform. Alternatively, the form attached as Annex A must be completed and emailed to dataservices@judicium.com.

Once notified, the GLT Data Protection Officer shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Further details may be required by the GLT Data Protection Officer from the school / service to make an assessment. Unless-the GLT Data Protection Officer concludes that there is unlikely to be any a risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the school Data Protection Lead

unless a delay can be justified. The GLT Data Protection Officer may require a further form to be completed and will provide this to the person making the report or the Data Protection Lead within the school / service.

Where a breach is determined as reportable, the GLT Data Protection Officer shall inform the Information Commissioner of:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries which shall be the GLT Data Protection Officer;
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Data Protection Lead within the school / service under the guidance and advice of the GLT Data Protection Officer shall notify data subjects of the breach without undue delay., unless the data would be unintelligible to those not authorised to access it or measures have been taken to mitigate any risk to the affected individuals.

The affected data subjects shall be informed of:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

4. Assessing The Breach

Once initial reporting procedures have been carried out, the school /service will carry out all necessary investigations into the breach.

The school Data Protection Lead will identify how the breach occurred and 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 insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the school / service 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 school / service; and
- Any other wider consequences which may be applicable.

5. Preventing Future Breaches

Once the data breach has been dealt with, the school Data Protection Lead will consider its security processes with the aim of preventing further breaches. In order to do this, they will: -

- 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 awareness within members of staff 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.
- Update the data breach register.
- Submit a report to the Headteacher who will report to the Governing Body.

All breaches will be reported to the Board of Trustees by the GLT Data Protection Officer and any recommendations for further training or a change in procedure shall be reviewed by the Board of Trustees and a decision made about implementation of those recommendations.

Reporting and monitoring

Reports on data breaches and summary data, with any recommendations with suggestions for further training or changes to policy will be reported regularly to the Board of Trustees or appropriate Committee.

Annex A – Judicium / ICO Data Breach Reporting Form

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

(Follow-up reports only) ICO case reference:

About the breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?

How did you find out about the breach?

When did you discover the breach?

Date:

Time:

When did the breach happen?

Date:

Time:

Categories of personal data included in the breach (tick all that apply)

☐ Data revealing racial or ethnic origin

☐ Political opinions

☐ Religious or philosophical beliefs

☐ Trade union membership

☐ Sex life data

☐ Sexual orientation data

☐ Gender reassignment data

☐ Health data

☐ Basic personal identifiers, eg name, contact details

☐ Identification data, eg usernames, passwords

☐ Economic and financial data, eg credit card numbers, bank details

☐ Official documents, eg driving licences

☐ Location data

☐ Genetic or biometric data

☐ Criminal convictions, offences

☐ Not yet known

☐ Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

☐ Employees

☐ Users

☐ Subscribers

☐ Students

☐ Customers or prospective customers

☐ Patients

☐ Children

☐ Vulnerable adults

☐ Not yet known

☐ Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

☐ Confidentiality

☐ Integrity

☐ Availability

(Cyber incidents only) Impact on your organisation

(Cyber incidents only) Recovery time

Had the staff member involved in this breach received data protection training in the last two years?

(Initial reports only) If there has been a delay in reporting this breach, please explain why

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature*

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, eg confirmed data sent in error has been destroyed, updated passwords, planning information security training.

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed*

Have you told data subjects about the breach?

Have you told, or are you planning to tell any other organisations about the breach?

eg the police, other regulators or supervisory authorities. In case we need to make contact with other agencies

If you answered yes, please specify

About you

Organisation (data controller) name

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name:

Email:

Phone: