DATA BREACH POLICY

1. ABOUT THIS POLICY

1.1 The corporate information, records and data of The Levels School Limited is important to how we conduct business and manage employees.

1.2 This Data Breach Policy explains how we manage data breaches.

1.3 Failure to comply with this policy can expose us to fines and penalties, adverse publicity, difficulties in providing evidence when we need it and in running our business.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. SCOPE OF POLICY

2.1 This policy covers all data that we hold or have control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings and CCTV recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as "data".

2.2 This policy covers data that is held by third parties on our behalf, for example cloud storage providers or offsite records storage. It also covers data that belongs to us but is held by employees on personal devices.

2.3 This policy applies to all business units and functions of The Levels School Limited.

3. GUIDING PRINCIPLES

3.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our business effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.
- We regularly monitor and audit compliance with this policy and update this policy when required.

4. DATA BREACH PROCEDURE

4.1 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:

- 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

4.2 When does a personal data breach need to be reported?

We must notify the Information Commissioners Office 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.

4.3 Reporting a data breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should immediately notify the data protection officer.

Breach reporting is encouraged by us 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, or the Data Protection Officer.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Data Protection Officer will acknowledge receipt of the data breach and take appropriate steps to deal with the report.

4.4 Managing and recording the breach

On being notified of a suspected personal data breach, the Data Protection Officer 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 our data breach register
- Notify the Information Commissioner's Office
- Notify data subjects affected by the breach
- Notify other appropriate parties to the breach
- Take steps to prevent future breach.

4.5 Notifying the ICO

The Date Protection Officer will notify the Information Commissioner's Office 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. If we 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 Information Commissioner's Office.

4.6 Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer will notify the affected individuals without undue delay including the name and contact details of the Data Protection Officer and Information Commissioner's Office, the likely consequences of the data breach and the measures we have (or intend) 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 we will consider alternative means to make those affected aware (for example by making a statement on our website).

4.7 Notifying other authorities

We 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)
- The Local Authority
- The police (for example if the breach involved theft of equipment or data)

4.8 Assessing the breach

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

We will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We 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, we will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the Information Commissioner's Office 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)
- 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 us
- Any other wider consequences which may be applicable

4.9 Preventing future breaches

Once the data breach has been dealt with, we will consider its security processes with the aim of preventing further breaches. In order to do this, we 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 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
- Update the data breach register
- Debrief Governors following the investigation
- Identify any trends in data breaches.

Prevention is always better than dealing with data protection as an afterthought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the Data Protection Officer. This can help capture risks as they emerge, protect us from data breaches and keep our processes up to date and effective.