DATA BREACH INCIDENT REPORTING POLICY

Learning Academies Trust

Version:	1.0		
Approved by:	Apex HR	Ratified date:	16th March 2023
Last review date:	22 November 2022	Next review date:	31st March 2024

LEARNING ACADEMIES TRUST

CONTENTS

1. Overview 2
2. Personal Data Breaches 3
3. Identifying a breach 3
4. Incident Reporting 4
5. Example Action to minimise the impact of data breaches. 4
6. Final Outcome of reporting breaches 5

CHANGES

Policy date	Summary of change	Author	Version	Review date
01/12/2018	Policy has been created	Apex HR Ltd	1.0	01/11/2019
22/11/2022	Reviewed	Apex HR Ltd	1.0	22/11/2023

1. OVERVIEW

1.1. This policy sets out the procedures and expectations to detecting data breaches, with respect to identifying breaches, responding to breaches and notification of breaches to supervisory authorities, data controllers and data subject, under the reviewed Data Protection Act 2018.

1.2. This policy and procedure will apply to all staff working within Learning Academies Trust (LAT), contractors, third party companies/agencies who process data where the LAT is the data controller or has an interest in the personal data affected.

1.3. Definitions within this policy

a) "DPO"- Appointed person acting as the Data Protection officer who oversees the dealing with the breaches affecting the company.

b) "Data Controller"- the legal person, public authority, agency or other body which determines the purpose and means of the processing of the personal data.

c) "Data Processor" legal person, public authority agency or other body which processes personal data on behalf of the controller.

d) "Data Subject" identifiable natural person, who can be identified either directly or indirectly through a range of data values.

e) "Personal Data (PD)" any information relating to a data subject.

f) "Supervisory authority" Information Commissioners Office (ICO)

1.4. Under Data Protection Act 2018, a personal data breach means there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. It also includes breaches that are the result of both accidental and deliberate causes. Examples of personal data breaches can include:

- Accessed by an unauthorised third party

- Deliberate or accidental action (or inaction) by a controller/processor
- Sending PD to an incorrect recipient
- Computing devices containing PD being lost or stolen
- Alteration of PD without permission
- Loss of availability of PD

1.5. A data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. As described above there will be a breach when PD has been lost, destroyed, corrupted or disclosed, this will include if someone has accessed the data or passes it on without authorisation or if the data is made unavailable and these actions has a negative effect on individuals. Examples of these are:

- Confidentiality Breach- where there is unauthorised or accidental disclosure or access to PD
- Integrity Breach- unauthorised or accidental alteration of personal data
- Availability Breach- unauthorised or accidental loss of access or destruction of PD

Examples of common breaches are listed below:

Type	Definitions
Technical	Data Corruption Malware Hacking Corrupt Code
Physical	Unescorted visitors in secure/unauthorised areas Break-ins to sites Thefts from secure sites Theft from unsecure vehicles/premises Loss in transit/post
Human	Non-secure disposal of hardware or paperwork Unauthorised disclosures Inappropriate sharing of personal data Data input errors Unauthorised access/users

2. PERSONAL DATA BREACHES

2.1. The LAT will endeavor to protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

2.2. The LAT will also take stringent steps to ensure that there are no personal data breaches and we will review our processes annually.

2.3. It is all of the staff's responsibility to ensure they take precautionary measures and are vigilant when dealing with data. The staff has a responsibility to adhere to policies and procedures when processing data, they must also participate and receive in regular updated training.

2.4. All staff have a responsibility to report breaches as soon as they are identified whether this has been caused by the individual staff member or identified from another source.

3. IDENTIFYING A BREACH

3.1. Although procedures are in place to avoid breaches and to ensure the upmost security of data, sometimes breaches do happen beyond our control. On finding and or causing a breach, or a potential breach, the staff member or data processor must inform the Data Protection Officer immediately.

3.2. The DPO must be informed via email, dpo@learningat.uk, with details of the breach and completing the incident reporting form, when it happened and the initial likely impact. The DPO will assess the report, investigate the breach and carry out a risk assessment based on the information provided.

3.3. The Appointed person or DPO with advice on reasonable steps to be made by the staff or the processor to contain the breach and minimise impact to individuals possibly affected.

3.4. The appointed person/DPO will make a decision on the severity of the breach. If the Breach is deemed to be low risk, a record of the breach must be made with a justification of the decision. If the breach is deemed to be medium to high risk, this will be required to be reported.

3.5. The DPO will then take steps to report to the Information Commissioners Office (ICO) within 72 hours and act on the advice of the ICO and submit a report. If the breach is large and it is likely to affect the rights and freedoms of individuals, a notification period will be set up and all individuals will be notified.

4. INCIDENT REPORTING

4.1. As we will try our upmost to avoid breaches, the ones that do get investigated, will be recorded on an incident report form. This will be a form detailing all relevant information relating to the breach, how it was dealt with, whether it was reported to ICO and notified to individuals. It will also evaluate risk level and justification for final decision.

5. EXAMPLE ACTION TO MINIMISE THE IMPACT OF DATA BREACHES.

5.1. To minimise impacts of any data breaches, there will be initial actions taken to reduce the impact of the breach, such actions will involve the reducing the breach of sensitive information, customer's information and non-anonymised data. Such actions are as follows:

- Special category (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they identify the error.
- Members of staff who received personal data in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact that publisher/website owner or administrator to request that the information is removed from their website and deleted.

Breaches will happen at some stage, whether they are large scale or minor, however it is essential that every step is taken to avoid these breaches and that a clear record of action is reported and maintained on how the breach was efficiently dealt with. All other actions against breaches will be assessed on a case by case basis.

6. FINAL OUTCOME OF REPORTING BREACHES

6.1. All breaches need to be reported at the earliest detection to the Data Protection Officer. Breaches should not be reported directly to the ICO or any of the affected data subjects without consulting the DPO in the first instance.

6.2. The DPO will then decide and consider if the breach has resulted in the risks to the rights and freedoms on the Data Subject, they will then escalate the breach incident further. Not all data breaches will result in formal action. Some may be false alarms or a Near miss, events that do not result in a risk to the rights and freedoms of the individuals. Other formal action that may not require to be reported to the ICO and will be decided as low risk and unlikely to affect the rights and freedoms of the Data Subject. Although these incidents result in no further action, they are still required to be recorded on the incident reporting sheet and justification made of final outcome.

6.3. All breaches must be investigated immediately and, where applicable further steps will be taken to and ensure containment, identify the risk and prevent recurrence.

6.4. Annual review of processes and procedures shall be carried out. This policy may be amended from time to time in accordance with updates from the Data Protection 2018 regulations.