# HLTY DATA BREACH POLICY AND PROCEDURES

THIS POLICY APPLIES TO THE HOPE TRUST BOARD, ALL TRUST SCHOOLS AND THE HOPE TEACHER TRAINING PARTNERSHIP

**Document Management:**
Date Policy Created: March 2017
Date Policy Approved: 25 November 2019
Date Amended:
Next Review Date: November 2020
Version: 2.0
Approving Body: Resources Committee

## Statement of Intent

**Hope Learning Trust York (HLTY)** has a duty under the General Data Protection Regulations (GDPR) to protect and regulate all personally identifiable data processing activities, and also report certain types of data breach to the Information Commissioners Office (ICO). This set of procedures is a response plan, put in place to ensure that all members of staff and the wider school/academy/Trust community recognise what constitutes a data breach and understand their personal responsibility to report **all** incidents as soon as they occur, regardless of severity.

**HLTY** ensures that all members of staff, Governors, Trustees and Members are given appropriate training in data protection procedures, to minimise the risk of data breach incidents occurring.

All data breach incidents are logged regardless of severity, and certain incidents must be reported to the ICO within 72 hours of discovery.

**HLTY** also have a duty to inform individuals of a breach of personal data if it is likely to result in a high risk to their rights and /or freedoms. This must be done without delay.

**Signed by:**

| | | | |
|---|---|---|---|
| _____ | **Chief Executive Officer** | **Date:** | _____ |
| _____ | **Chair of Resources Committee** | **Date:** | _____ |

## 1. Definitions

For the purpose of this policy, '**personal data'** refers to personal information that could identify a living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

**'Sensitive personal data'** is referred to in the GDPR as 'special categories of personal data' which are broadly the same as those in the Data Protection Act (DPA) 1998 These specifically include the processing genetic data, biometric data and data concerning health matters, ethnicity, religion and sexual orientation.

**'Personal 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.

## 2. Consequences

The consequences of a Data Breach under GDPR for the Trust will vary dependent upon the severity of the breach.

In short, the ICO are entitled to fine an organisation **up to 2% of the annual turnover, or 10 million euros, whichever figure is higher** for a 'low risk' breach, and **up to 4% of the annual turnover or 20 million euros, whichever figure is higher** for a serious breach in which the rights or freedoms of individuals has been severely compromised.

Failing to notify a breach when required to do so can also result in a significant fine up to **10 million euros or 2 per cent of your global turnover.**

A data breach may also open the school and Trust to risk of legal action for which data subjects may be entitled to monetary compensation.

## 3. Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- General Data Protection Regulation (GDPR)

## 4. Scope

This set of Data Breach procedures applies to all staff, Contractors, Governors, Trustees and Members of **HLTY**, Trust Schools and EborHope Teaching School Alliance.

All staff and members of the Trust community have a role to play to ensure a safe and secure workplace, and to ensure compliance with data protection of individuals under GDPR. Training will be provided to all members of staff, governors, Trustees and Members to mitigate the risks of a data breach, and to ensure that individuals understand their personal responsibility to:

- Protect personal data

- Report a breach of personal data without delay

## 5. Incident Management

A Data Protection breach is the result of an event or series of events where personally identifiable data is exposed to unauthorised or inappropriate processing that results in its security being compromised. The extent of damage or potential damage caused will be determined by the volume, sensitivity and exposure of the data breached.

Breach management is concerned with detecting, reporting and containing incidents with the intention of implementing further controls to prevent the recurrence of the event.

A non-exhaustive list of examples of potential data breaches are summarised below.

| Type | Example |
|---|---|
| Technical | Data Corruption<br>Malware<br>Corrupt Code<br>Hacking |
| Physical | Unescorted visitors in secure areas<br>Break-ins to sites<br>Thefts from secure sites<br>Theft from unsecured vehicles/premises<br>Loss in transit/post |
| Human Resources | Data Input errors<br>Non-secure disposal of hardware or paperwork<br>Unauthorised disclosures<br>Inappropriate sharing |

## 6. Possible Scenarios

- A teacher leaves their computer logged on and unlocked; a pupil finds the phone number and address of a member of staff
- An assistant headteacher leaves their memory stick or external hard drive on the bus or in a café
- Someone emails a pupil list with dates of birth and SEND details using their personal email account
- Someone has their laptop stolen from their car
- An email is sent out to a group of parents without using the 'blind carbon copy' (Bcc) function; all email addresses are visible to all parents within the group
- A photograph of a pupil is published on a school Twitter account with their full name in the caption.
- A rewards data file with pictures of pupils alongside their name and school name was on an external hard drive which has been lost.

## 7. Process for reporting incidents

See Appendix A for the flow of action required from first discovery of a potential data breach to its final conclusion.

- The employee, **must** in the first instance, report **any** data breach to the **Designated Data Protection Controller** at their school/academy **IMMEDIATELY**
- If the Data Protection Representative is not immediately available, the employee MUST report direct to **HLTY Data Protection Officer (DPO), Wendy Munro** on **07713 385382.**
- **This is a 24 hour, 7 days a week service. It is imperative that the breach is reported as soon as it is discovered.**
- Employees of HLTY are **legally obligated** to report the incident **immediately**.

### DISCOVERY & REPORT

EMPLOYEES: All breaches and weaknesses need to be reported urgently and at the earliest possible stage to the **Data Protection Controller OR** direct to the **DPO Wendy Munro** by telephone on **07713 385832 (24 hour service).**

If reported to the **Designated Data Protection Controller** in school, they **must** then report direct to the **DPO Wendy Munro** by telephone on **07713 385382 without delay (24 hour service).**

### IDENTIFY AND RECORD

Following notification, the **DPO** will record the incident on the **HLTY** Data Breach Log and make an initial assessment of the breach's severity. At this point the **DPO** will decide if there is a need to send an early report of the breach to the ICO.

The Data Breach Log should capture most of the information needed to establish the scope of a breach but there will be a need to obtain additional information about the event, the data affected, determining the type of incident, its category and priority before putting together a full report.

### ASSESS AND INVESTIGATE

The data breach will be assessed to determine the type and quantity of data involved, level of sensitivity, whether it is protected/encrypted, whose data has been compromised and how, and also what actions have been taken to protect it. This is achieved by interviewing the key personnel involved in the breach and their line managers and collecting as much information as possible.

At this point, the **DPO** will mitigate potential harm to individuals or the school community; this could include physical safety, emotional wellbeing, reputation, finances, identity or private affairs, and any threats to public reputation or general operations.

### REPORT TO ICO

The **DPO** is responsible for reporting data breaches to the ICO. Recital 87 of the GDPR makes clear that when a security incident takes place, the **DPO** should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required. All incidents which are required to be reported to the ICO must be done without delay and at least within 72 hours of discovery. Failure to report a breach when required is subject to a fine of 10 million euros or 2% of global turnover, whichever is highest.

Not all data protection breaches will result in a report to ICO. Some will be false alarms or "near miss" events that do not pose a risk to the rights and freedoms of individuals. These should still be reported, as all incidents of data breach must be recorded on the Data Breach Log.

## REPORT TO DATA SUBJECTS

The **DPO** will assess the severity of the breach in relation to the rights and freedoms of the data subjects affected. At the time of reporting to the ICO, the **DPO** will also decide if the data subjects should be informed of the breach, and if so this must be done without delay. If necessary, the **DPO** will notify third parties (e.g. police).

## LEARN

Evaluation will include the root of the breach and where any current or future risks like. The **DPO** will identify any weak points in existing security measures and procedures and recommend appropriate measures for the future. The **DPO** will also identify weak points in security awareness and training among staff and recommend new strategies and processes.

The **DPO** will report on assessment findings to the Senior Leadership Team. The purpose of the report is to document the circumstances of the breach, what actions have been taken, what recommendations have been made and whether the disciplinary action process needs to be followed.

Key to preventing further incidents is ensuring the organisation learns from an incident. Regular review meetings will take place chaired by the **DPO** to agree recommendations and each Breach Report will be shared with Senior Leadership Team and the Local Governing Committee (LGC).

## TRAINING

During the assessment of Data Protection processes, further training opportunities may be identified following the breach; training and staff briefing sessions may be implemented to effectively address and mitigate risks to data security.

**Review and Revision**

This document will be reviewed and updated at regular intervals as appropriate, and annually.
Next review due: **November 2020.**

**Key Message**

A culture in which data protection breaches are reported should be fostered. Although sanctions cannot be totally ruled out, the key objective is to develop valuable insight into how such events occur and staff need to be assured that reporting a breach will not in itself result in disciplinary action.

**Appendix A**


Contact **HLTY Data Protection Officer (DPO), Wendy Munro on**

**07713 385382**

**(24 hour on-call service)**