6 principles in Art.10 GDPR

Personal data must be:-

1	**processed lawfully, fairly and transparently**	**lawfulness, fairness and transparency**
2	collected for specific, explicit and legitimate purposes	purpose limitation
3	adequate, relevant and not excessive	data minimisation
4	accurate and up to date	accuracy
5	Kept no longer than necessary	storage limitation
6	processed securely	integrity and confidentiality

Data Breach Procedure
for Healing Multi-Academy Trust Schools

Policy Statement

Healing Multi Academy Trust Schools hold large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by Healing Multi Academy Trust Schools [Healing School, A Science Academy, Healing Primary School, Great Coates Primary Academy, William Barcroft Junior School, St Giles Academy, Woodlands Academy, Hartsholme Academy, Lincoln Castle Academy & Ermine Primary Academy]. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Healing Multi Academy Trust Schools if a data breach takes place.

Legal Context

Principle 7 of the GDPR Act states that organisations which process personal data must take

"appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Types of Breach

Data Protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or governing body data and/or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as fire or flood
- Hacking
- 'Blagging' offences where information is obtained by deception.

6 principles in Art.10 GDPR

Personal data must be:-

1	**processed lawfully, fairly and transparently**	**lawfulness, fairness and transparency**
2	collected for specific, explicit and legitimate purposes	purpose limitation
3	adequate, relevant and not excessive	data minimisation
4	accurate and up to date	accuracy
5	Kept no longer than necessary	storage limitation
6	processed securely	integrity and confidentiality

Reporting

If you discover that data has been lost, or if you believe there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the Data Protection Officer (DPO@healingmultiacademytrust.co.uk) and Principal/Headteacher. The priority must then be to close or contain the breach to mitigate/minimise the risks to those individuals affected by it.

Consider the following points:

- Containment and recovery
- Assessment of on-going risk
- Notification of breach
- Evaluation and response

Containment and recovery

1. The person who discovers/receives a report of a breach must inform the Principal/Headteacher of the school and the Trust DPO. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the Data & Networks Manager.
3. The DPO & Trust CEO must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the Trust's responsibility to take the appropriate action and conduct any investigation.
4. The breach must be logged on the GDPR.co.uk software under the 'Data Breaches' section.
5. The DPO and Trust CEO must also consider whether the ICO need to be informed, within the specified 72 hours.
6. The DPO, CEO & Principal/Headteacher must quickly take appropriate steps to recover any losses and limit the damage.

Assessing the risks

Level of risks can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen.

- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?

6 principles in Art.10 GDPR

Personal data must be:-

1	**processed lawfully, fairly and transparently**	**lawfulness, fairness and transparency**
2	collected for specific, explicit and legitimate purposes	purpose limitation
3	adequate, relevant and not excessive	data minimisation
4	accurate and up to date	accuracy
5	Kept no longer than necessary	storage limitation
6	processed securely	integrity and confidentiality

- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in an important service provided?

Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.

Notification of breaches

- Inform the Trust DPO, Principal/Headteacher immediately or within 24 hours of being made aware of the breach with your name, the date/time of breach, date/time you detected it and give basic information about the type of breach and information about personal data concerned. Include details of what you have already done to respond to the risks posed by the breach.

- The DPO may ask you questions about what has occurred to ascertain any further actions including whether the breach qualifies for immediate notification to the ICO or not.

- The DPO will assess the type and level of risk and, if necessary, inform the ICO.

- The ICO, whom if necessary will be informed by the DPO, will investigate the breach in their capacity as the independent regulator for Data Protection.

Evaluation and response

It is important to investigate causes of the breach and also evaluate the response effectiveness.

Simply containing the breach and continuing business as usual is not acceptable.

You can discuss further prevention of breaches with the Trust Data Protection Officer: DPO@healingmultiacademytrust.co.uk