Record keeping

5.1.2 GDPR compliance: Data breach management policy

Steps to take in the event that there is a breach of GDPR rules on personal data.

1. Assess the risk

Upon discovering a data breach you should begin by assessing the risk it could pose. You need to consider if the breach could cause any **harm** to individuals.

When evaluating the risk you need to consider:

- How **sensitive** is the data? Special category data probably poses a greater risk if breached than just first names, for example.
- How **many** data subjects are affected? A breach involving only one individual is probably a lower risk than one involving a much larger number.
- Could the breach lead to **distress**, or **physical harm**? How likely is this?
- Are there any **safeguards** in place that could lower the risk? For example, an encrypted memory stick is a lower risk if lost than an unencrypted memory stick would be.
- Are there more safeguards you can put in place now? For example, could a lost device be remotely wiped or locked? Could you now change your password to prevent further access to personal data?

2. Report the incident

If you become aware of a breach you should immediately notify your school Data Protection Officer (DPO), or the designated person in your school's data breach procedure.

If East Sussex County Council are your DPO then please refer any breaches to the ESCC Information Governance team ASAP. In most cases school staff should report breaches to their Business or Office Manager who can then pass the details on to the Information Governance team. Make sure you are familiar with the reporting process in your school.

There is a 72 hour window for reporting serious breaches to the ICO so reporting the incident needs to be done quickly.

3. Contain the breach

Once a breach has been discovered and reported, you next need to take steps to contain the breach and limit the damage.

Examples of containing a breach could include:

- Changing passwords
- Contacting parents

- Recovering/recalling letters
- Remotely locking/deleting data from a device (if possible)

4. Decide who else you need to inform

As well as informing your school DPO there are several other people you may need to inform in the event of a breach, including:

- Other relevant organisations e.g. the police (if there is an immediate risk of harm from the data breach) or banks (if personal financial information has been breached).
- The data **subjects** affected. Article 34 of the UK GDPR states you must notify data subjects that their data has been breached if "it is likely to result in a high risk to their rights and freedoms". However many schools will choose to notify data subjects in the event of all breaches, as it may be better for them to hear about a breach from the school rather than, for example, another parent in the playground who received their data in error.

5. Learn from the incident

The ICO are very keen to see that learning has taken place following a breach. This is vital as it is the means by which schools can develop their policies and procedures to minimise the risk of similar breaches happening again.

Under the UK GDPR, nurseries should keep a central record of **all** breaches, regardless of whether they were reported to the ICO, and any learning or developments that have been implemented as a result.

This advice was taken from ESCC training on GDPR.

This policy was adopted on	**Signed on behalf of the nursery**	**Date for review**
09/08/23	Stuart Watt	01/08/24