



Personal Data Breach Procedure

Summary

Meadow Learning CIC (The Meadow) processes personal data, including special category personal data about young people. It is essential that procedures are in place to keep any threat to that information to a minimum, and that any breach is identified and put right quickly. Any incident that compromises the security of that information, or the systems it is held in, must be managed in line with the law and guidance from the Information Commissioner's Office (ICO).

This procedure aims to:

- reduce the impact of information security incidents by making sure they are followed up correctly
- make sure serious incidents are reported to the right external organisations
- help us learn from incidents so that they are less likely to happen again.

Our **Data Protection Lead** is Claire Imhasly (Manager and Director), and she is the key point of contact for personal data breaches. If the Data Protection Lead is unavailable, report to Debbie Forster (Director).

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. In short, there is a breach whenever personal data is lost, destroyed, corrupted or disclosed; if someone accesses it or passes it on without proper authorisation; or if it becomes unavailable and that has a significant effect on people. Examples include:

- giving information to someone who should not have it, verbally, in writing or electronically
- theft or loss of a phone, laptop or paper records
- sending personal data to the wrong person, or a message to all parents by mistake
- writing down a password and leaving it where it can be found
- printing or copying confidential information and not storing it securely
- safeguarding information being seen by someone who should not see it
- a computer or account being infected by a virus or other malware, or signed into by someone else
- finding information that has been changed by someone without permission
- using unapproved apps or software with Meadow accounts.

What to do

If you know or suspect that a breach has happened:

1. **Tell the Data Protection Lead straight away.** Do not try to investigate it yourself, and keep any evidence.
2. The Data Protection Lead takes immediate steps to contain the breach, for example asking the recipient of a misdirected email to delete it, signing a lost phone out of Meadow accounts and changing passwords, or retrieving lost paper records.
3. The Data Protection Lead informs the directors.
4. **If the breach involves information about a young person placed by a school or the local authority, we tell that school or the local authority the same day.**
5. If the breach involves safeguarding information, the Designated Safeguarding Lead is also informed and considers whether any child is at risk.

Investigation and reporting

The Data Protection Lead checks whether the information has been made public (for example online) and, if so, asks for it to be removed.

She then assesses how serious and how likely the consequences are, including the risk of: loss of control over their data; discrimination; identity theft or fraud; financial loss; damage to reputation; loss of confidentiality; or any other significant disadvantage or distress.

If the breach is likely to put people's rights and freedoms at risk, the Data Protection Lead reports it to the ICO within 72 hours of becoming aware of it, using the ICO's online breach report. The report sets out:

- what happened, the types and approximate number of people and records involved
- the name and contact details of the Data Protection Lead
- the likely consequences
- what has been done, or will be done, to deal with the breach and reduce its effects.

If not all the details are known within 72 hours, we report what we know and send the rest as soon as possible.

If the risk to people is high, we also tell the people affected promptly, in writing, explaining what happened, the likely consequences, what we are doing about it and who to contact.

Recording

The Data Protection Lead records every breach, whether or not it is reported to the ICO, including the facts and cause, the effects, the decision on reporting and why, and the action taken to contain it and stop it happening again. Breach records are kept securely in our restricted Google Drive.

Review

After any breach, the Data Protection Lead and the directors review what happened as soon as possible and agree changes, such as better processes or more training.

Security weaknesses and events

Everyone must report security weaknesses and events to the Data Protection Lead in the same way, for example:

- suspicious sign-in alerts or repeated account lock-outs
- password sharing or other misuse of access
- a lost or unlocked device

- viruses or other malicious software
- not following our Information Security and Acceptable Use Policy.

Do not try to test or prove a weakness yourself. If a weakness is reported to a provider such as Google or WhatsApp, tell the Data Protection Lead as well.

Contact

Claire Imhasly, Data Protection Lead · themeadowbath@gmail.com · 07411 865399

Reviewed: October 2026 · **Approved by:** the Directors of Meadow Learning CIC · **Next review:** October 2027, or sooner if law or guidance changes