DATA PROTECTION

TO PRINT – CLICK HERE

All organisations including early years settings which handle personal information about individuals must ensure that they follow the guidelines set down by the General Data Protection Regulation.

The General Data Protection Regulation (GDPR) standardizes data protection law across all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information (PII).

GDPR replaces the 1995 EU Data Protection Directive, and came into force on May 25, 2018 and the changes remain in place even after the UK leaves the EU in 2019.

GDPR gives individuals greater control over their own personal data.

Early Years settings may already have a data protection policy in place but GDPR introduces some significant changes in what is needed.

GDPR principles

GDPR condenses the Data Protection Principles into six areas, referred to as the Privacy Principles. They are:

1. You must have a lawful reason for collecting personal data and must do it in a fair and transparent way.
2. You must only use the data for the reason it is initially obtained.
3. You must not collect any more data than is necessary.
4. It has to be accurate and there must be mechanisms in place to keep it up to date.
5. You cannot keep it any longer than needed.
6. You must protect the personal data.

These privacy principles are supported by a further principle – accountability.

This means your setting must not only do the right thing with data but must also show that all the correct measures are in place to demonstrate how compliance is achieved.

There is also an expectation that staff will be trained on data protection. Documentation on policies, procedures and training is going to be a key part of any effective compliance programme.

Areas to consider

Appointing a data protection officer — For most settings, appointing an individual who takes the lead on data compliance will be enough, although for larger early years provider chains may need to appoint a data protection officer.

Privacy notices — When you collect any data you must tell people exactly how you are going to use it, who might you share it with, how long you will keep it as well as information on consent and complaint.

Individual rights — People now have new and enhanced rights on the collection, access and deletion of their data so you must ensure your setting has mechanisms to allow individuals to exercise these rights.

Consent — GDPR requires early years providers to have a legitimate reason for processing any personal data. Where you rely on consent for processing data you must be able to demonstrate that the consent was freely given. Pre-ticked boxes or inactivity will no longer suffice. People have to actively opt-in.

Data agreements — Early years providers are now obliged to have written arrangements with anybody processing data for them. Providers must make sure that anyone processing data meet GDPR requirements.

New projects — Data protection must be incorporated into new projects and services at the development stage — not simply as an after-thought.

Breach notification — You are obligated to notify the Information Commissioner's Office (ICO) of a data breach within 72 hours of becoming aware of the breach.

Fines — One of the key drivers of compliance is that organisations can be fined significant amounts if they are not. However you should focus on the benefits of ensuring you are handling your data properly.