GDPR in Early Years and Childcare settings

What’s the connection? Data Protection

25th of May 2018
What is GDPR?

Test your knowledge
10 minute quiz
Think of GDPR as evolutionary, not revolutionary
Why?

GDPR legislation replaces the current Data Protection Act

GDPR comes into force on 25th May 2018
What have you heard?

- Lots of complex issues?
- Huge amounts of work?
- Huge fines if you get it wrong?
GDPR in Summary

- New EU legislation
- Replaces Data Protection Act 1998
- GDPR provides enhanced rights for data subjects (individuals) and holds data controllers to a higher standard when processing personal data
- Data Protection Bill will repeal DPA and incorporate GDPR after Brexit
What is the key difference between DPA and GDPR?

DPA: Compliant until proven not to be

GDPR: Must prove compliance from day 1
Data Protection now and post May 2018

- Legislation that sets out principles on how every organisation collects and uses personal data.

- Personal data is anything that relates to an identifiable, living individual.

- From details in info systems, to emails, paper files, CCTV, audio recordings, photographs etc.
Basic Terms

**DPA** – Data Protection Act 1998

**GDPR** – General Data Protection Regulation 2016

**Personal Data** – identifies a living individual

**Sensitive (Special) Personal Data** – Health, Religion, Sexuality, Ethnicity

**Data Subject** – the individual whose data is processed – *children & staff*

**Data Controller** – Decides how data is used and is accountable – *your school*

**Data Processor** – Uses the data under instruction from the Data Controller

**Processing** – anything you do with data

**Information Commissioner’s Office (ICO)** – the UK’s independent body set up to uphold information rights
The 6 GDPR Privacy Principles
(Condensed from the DPA Data Protection Principles)

1. Lawfulness, fairness and transparency
2. Purpose Limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality

Accountability: ‘The controller (provider) shall be responsible for, and be able to demonstrate compliance with the principles’

GDPR provides a Framework for organisations
12 steps to prepare for GDPR

Step 1 – Raise Awareness
Appoint GDPR lead to identify areas of the organisation that could cause compliance issues under GDPR

Step 2 – Review the information you hold
Document what information your organisation holds by carrying out an information audit

Step 3 – Communicate privacy information
Review current privacy notices and ensure they set out what information you request and why. Use clear and plain language and include:
Retention period / legal basis and purpose for processing data / complaints process / data subjects right to withdraw
12 steps to prepare for GDPR

Step 4 – Individual rights
Ensure your procedures cover all rights of individuals, including how you delete personal data or provided data electronically

Step 5 – Subject Access Requests
Update procedures to take new rules for access requests into account. Organisations can no longer charge (unless request is excessive), and you will have 1 month to comply as opposed to the current 40 days

Step 6 – Lawful basis for processing personal data
Identify the lawful basis for the organisation’s processing activity and update your privacy notice to include this
12 steps to prepare for GDPR

Step 7 – Consent
Review how you seek, record and manage consent and whether changes need to be made. Refresh existing consents if they do not comply with GDPR.

Step 8 – Children
Review how you verify children’s ages and obtain parental/guardian consent for processing activity.

Step 9 – Data Breaches
Make sure you have procedures in place to detect, report and investigate a personal data breach. Data breaches must be reported to the ICO within 72 hours and in some cases the individual affected.
12 steps to prepare for GDPR

Step 10 – Data Protection by design & data protection impact statements
Consider how your organisation will be using personal data before you start collecting it

Step 11 – Data Protection Officers
Designate someone to take responsibility for data protection. Decide and record whether you are required to appoint a data protection officer

Step 12 – International
Only a requirement if your organisation operates in more than one EU member state
So how do we get ready for GDPR?

- Complete the ICO’s self assessment checklist ‘Getting Ready for the GDPR’
- Complete your own information audit
- Develop policies and procedures including data breach, record retention periods
- Develop privacy notice and consent forms
- Ensure all staff are aware of GDPR
Further advice and guidance

- www.ico.org.uk

- https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf - Preparing for General Data Protection Regulations (GDPR) 12 steps to take now

- ICO helpline - 0303 123 1113

Case Studies