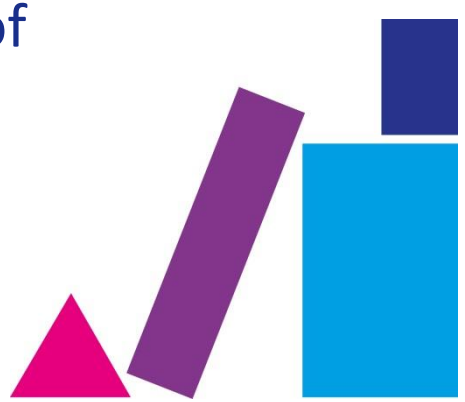
Early Years Scotland

Investing in our youngest children

Early Years Scotland
Investing in our youngest children

Open Badge in partnership with SSSC: GDPR Aware

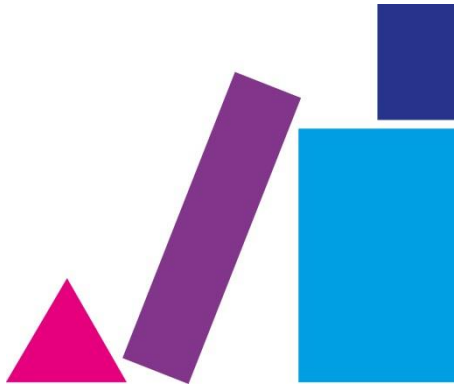
This Open Badge is informed by guidance available from the Information Commissioner's Office. This resource will raise your awareness of ensuring compliance within the regulation.



Early Years Scotland
Investing in our youngest children

What's New: General Data Protection Regulation (GDPR)

- The GDPR sets a high standard for consent, but the biggest change is what this means in practice for consent mechanisms.
- The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires individual ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.
- You **must** keep clear records to demonstrate consent.



What first? – A Data Audit

- Settings should consider how they collect information, how they process it, how it is stored and who engages in all elements of the process; this will ensure compliance.
- This audit of information must be carried out with both paper and electronic personal data.

What would this look like within your organisation?

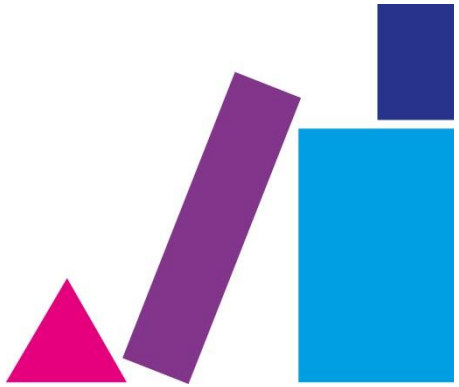
Early Years Scotland
Investing in our youngest children

Data Controller/Data Processor

- **Data Controller** – someone who determines the purpose and how any personal data is processed or will be processed.

- **Data Processor** – an individual who processes the data on behalf of the data controller.

- A Data Protection Officer **must** be appointed



Organisations will hold a diverse range of data for staff, families/children and other partners, examples are as follows:

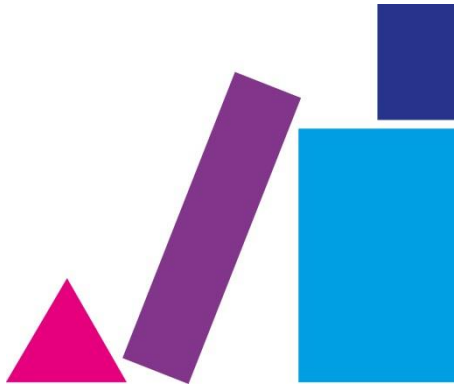
- Personal details, this will include details for all service users
- Family, lifestyle and social circumstances
- Education and training details
- Employment details
- Financial details

This is not an exhaustive list.

Systems used to hold data

- All personal data held in electronic format or contained within a structured manual filing system should be audited.
- In particular, but not exclusively, the audit should cover personal data held in the following systems and formats: -
- Computer databases
- Document management systems
- Individual computer files where appropriate e.g. spreadsheets and word-processed lists
- Structured e-mail directories
- Photographs

This is not an exhaustive list.

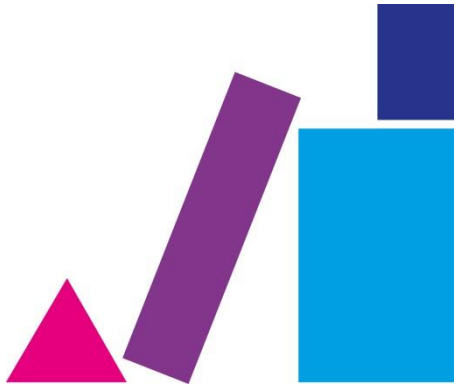


Data you may hold

In the case of settings who provide care for children, here are some examples of data you may hold:

- Children personal files
- Safeguarding records
- Family contact information
- Medical records

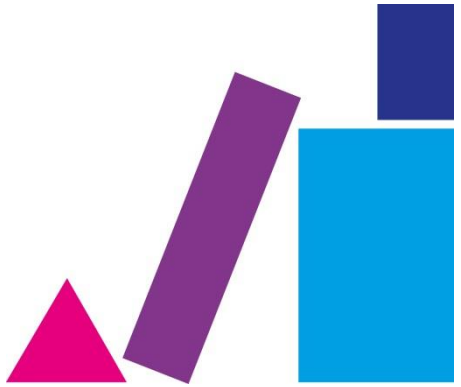
Again, this is not an exhaustive list. Completion of your data audit will identify all personal data you process.



Early Years Scotland
Investing in our youngest children

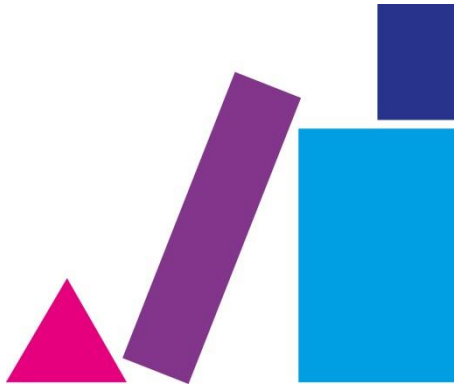
Eight Principles of Personal Data:

- Fair and Lawful Processing
- Lawful, clear and specific purposes
- Adequate and minimum necessary data
- Accuracy of data
- Retention of data
- The data subject's rights
- Appropriate security measures
- Transferring personal data oversees



Suggested audit questions:

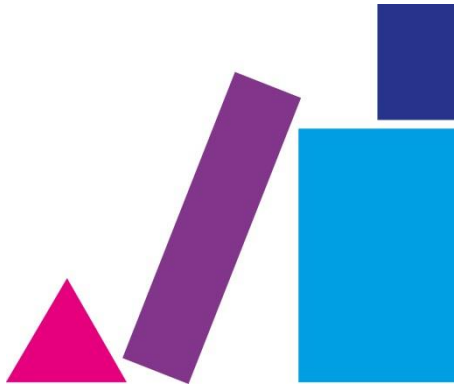
- Are you processing personal data?
- Are you processing sensitive personal data?
- Is personal data of children collected and processed?
- Is personal data only used for the purposes for which it was originally collected?
- How is consent given for the collection and processing of personal data and sensitive personal data?



Consent

- The GDPR gives a specific right to withdraw consent. You need to tell people they have rights in regards to their data. Individuals can withdraw consent at anytime and you must make this clear to them.
- You will be required to review your existing consent processes to check they meet the GDPR guidance.
- You may find that you will not have to make any significant changes to the consents you hold.

One of the main features of the regulation is to respect the rights of the individual through transparency and effective communication.



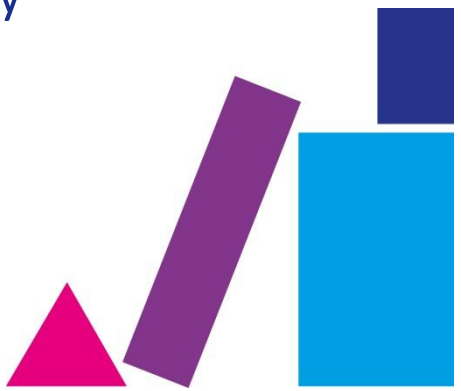
Early Years Scotland
Investing in our youngest children

Why is consent important?

- Consent is one lawful basis for processing (consent is most likely to be the appropriate lawful basis for processing data, see the ICO website for further advice on this).

- Genuine consent should put individuals in control, build customer trust and engagement, and enhance your reputation.

- Relying on inappropriate or invalid consent could destroy trust and harm reputation.



When is consent appropriate?

- Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.
- If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis (to maintain the relationship with your service users, it is most likely that you will require a significant amount of personal data).
- Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given (your consent processes should communicate clearly, why you need consent to hold personal data).

What is valid consent?

- Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.
- Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly
- Consent must specifically cover the controller's name, the purposes of the processing and the types of processing activity.
- Explicit consent must be expressly confirmed in words, rather than by any other positive action.
- There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

Early Years Scotland
Investing in our youngest children

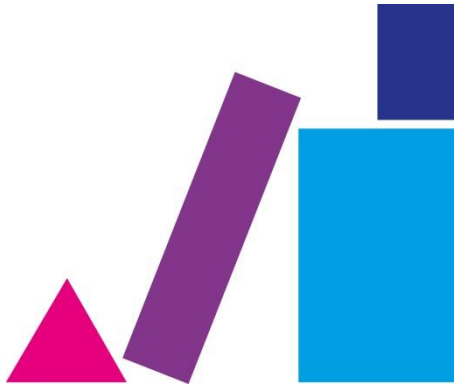
How should you obtain, record and manage consent?

- Make consent request prominent, concise, separate from other terms and conditions, and easy to understand.
- Include: the name of organisation; the name of any third party controllers who will rely on the consent; why the data needed; what will be done with it; and that individuals can withdraw consent at any time.
- Keep records to evidence consent – who consented, when, how, and what they were told.
- Make it easy for people to withdraw consent at any time they choose.
- Keep consents under review and refresh them if anything changes. Build regular consent reviews into business processes.

Early Years Scotland
Investing in our youngest children

Privacy Notice: employees

- A privacy notice will be required for employees (this can also include board of directors, volunteers, students and committee members)
- The notice will advise **what** and **why** data is collected
- You must make it clear what data is not mandatory
- If you plan to share any data with a third party you must ensure staff know this and have the option to opt out with no detriment
- Individuals must be aware of their right to access their personal data at any time



Early Years Scotland
Investing in our youngest children

Privacy Notice: parents/children

- A privacy notice will be required in relation to children in the setting
- The notice will advise what personal data is held, both that of children and families
- The notice will advise why personal data is held, both that of children and families
- Transparency is essential in how data is stored. Parents/carers must be informed of their rights in accessing data held on their family
- Consent rquires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.

Getting ready for the GDPR

We have replaced our Getting ready for the GDPR checklist with two new checklists - one for data controllers, and another for data processors.

Before undertaking our self assessment checklist to help your organisation get ready for the GDPR, you should first determine whether your organisation processes personal data as a "data controller" or "data processor". The definition of these two terms can be found in the Guide to the GDPR.

In some instances, organisation will process personal information as both a controller and a processor. When this is the case, we would advise you complete both assessments.

GDPR checklist for data controllers

Designed to help you, as a data controller, assess your high level compliance with data protection legislation. Includes the new rights of individuals, handling subject access requests, consent, data breaches, and designating a data protection officer, under the upcoming General Data Protection Regulation.

Start now

Early Years Scotland
Investing in our youngest children

GDPR checklist for data controllers

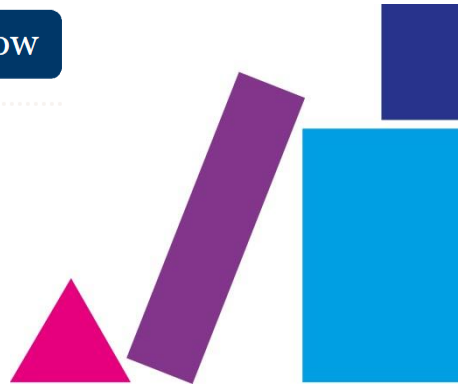
Designed to help you, as a data controller, assess your high level compliance with data protection legislation. Includes the new rights of individuals, handling subject access requests, consent, data breaches, and designating a data protection officer, under the upcoming General Data Protection Regulation.

Start now

GDPR checklist for data processors

Designed to help you, as a data processor, understand and assess your high level compliance with data protection legislation. Includes the new requirements for data processors, the rights of individuals, data breaches, and designating a data protection officer, under the upcoming General Data Protection Regulation.

Start now

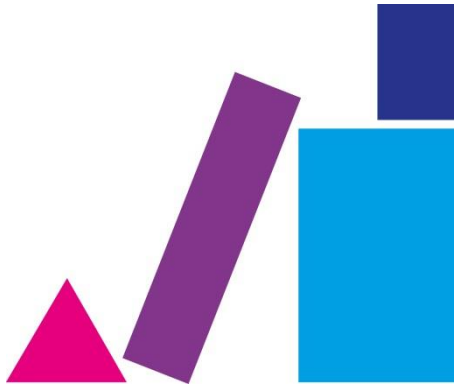


Early Years Scotland
Investing in our youngest children

Keeping up to date with GDPR

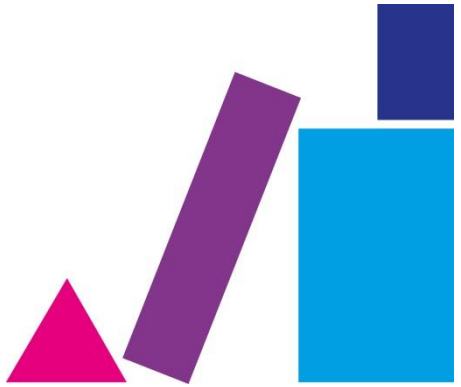
You must ensure you have a planned approach to GDPR compliance (this includes regularly reviewing your processes).There are a number of ways to do this. Some examples are:

- Visit the ICO website
- Access the Commissioner's Blog
- Call the ICO Helpline
- Engage in an ICO Live chat
- Follow the ICO Twitter feed



Links to ICO information provided:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/data-controllers/



Consent Checklist

Early Years Scotland
Investing in our youngest children

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Responsibility	Comments in relation to your role
We have checked that consent is the most appropriate lawful basis for processing.	
We have made the request for consent prominent and separate from our terms and conditions.	
We ask people to positively opt in.	
We don't use pre-ticked boxes or any other type of default consent.	
We use clear, plain language that is easy to understand.	
We specify why we want the data and what we're going to do with it. We give individual ('granular') options to consent separately to different purposes and types of processing	
We give individual ('granular') options to consent separately to different purposes and types of processing	
We name our organisation and any third party controllers who will be relying on the consent.	
We tell individuals they can withdraw their consent	
We ensure that individuals can refuse to consent without detriment.	
We avoid making consent a precondition of a service.	
If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.