London Borough of Waltham Forest

General Data Protection Regulations (GDPR) and Confidentiality Procedure

Early Years, Childcare & Business Development Service

LBWF Early Years, Childcare & Business Development Service have written this document to help you write a confidentiality policy for your setting. This document is for reference only and you must adapt it to reflect the service your setting offers. To download guidance on other policies and procedures go to https://thehub.walthamforest.gov.uk/

Whenever we say parents in this document we mean parents and carers and whenever we say child we mean children and young people aged 0 to 19 years old (up to 25 years old for young people with Special Educational Needs and Disabilities (SEND)).

Aim

Do you share information with parents and children? Do you make sure that parents and children can share information with you and can be confident that information shared will only be used for the benefit of their child? Do you make sure that any information you share is done so whilst respecting the privacy of children and their parents?

GDPR Principles

GDPR condenses the Data Protection Principles into 6 areas, which are referred to as the Privacy Principles:

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

Points to consider

- Introduction and scope of policy
- Definitions
- Roles and responsibility
- Personal Data Protection Principles
- Sharing personal data
- Subject access requests and other rights of individuals
- Biometric recognition systems (where applicable)
- CCTV (where applicable)
- Photographs and videos (where applicable)
- Record Keeping
- Accountability, Data protection by design
- Data security and storage of records
- Disposal of records
- Personal data breaches
- Training

- Review and Monitoring arrangements
- Providers must ensure that there is an area where staff may talk to parents and/or carers confidentially (Statutory Framework for the EYFS 3.61).

- Records must be easily accessible and available (with prior agreement from Ofsted, these may be kept securely off the premises). Confidential information and records about staff and children must be held securely and only accessible and available to those who have a right or professional need to see them. Providers must be aware of their responsibilities under the Data Protection ACT (DPA) 1998 and where relevant the Freedom of Information Act 2000 (Statutory Framework for the EYFS 3.69).

- How and where is information stored?

- Who has access to personal records?

- How long is information retained for?

- What type of records do you need to keep at your setting? Think about personal records for children and their families, staff records and so on.

- What will you include in the child's records? Think about observations, samples of work and achievements, Individual Support Plans (ISPs) and so on.

- Where will you store the children's development records and who will have access to them? Remember confidentiality.

- What information do you need to store in the personal records for the child and their family? Who can access these and how?

Children's Act Regulations – You must keep records of the name, address and date of birth of each child and the name, address and contact number of a parent. Consider who should have access to this information.

- Do you make staff aware that when they are discussing a child, confidentiality should take priority? Think particularly about when you are talking with parents or other staff in the setting.

- Where do you store staff personal details and employment issues? Consider that contracts and conditions of employment should remain confidential. Think about who should have access to this information, for example, line managers

- Appointing a data protection officer

- Privacy notices

- Individual rights

- Consent

- Data agreements

Cyber Security

Early Years education and childcare settings, like most other work environments, are increasingly reliant on technology.

That's why it's more important than ever to take steps to protect these devices (and the data we store on them) from accidental damage, or from online criminals. And it's also why **cyber security** is important to **all** of us. Cyber security is about safeguarding the devices we rely on, and protecting the services that all businesses, large and small, need to function.

Find out more about how to protect sensitive information about your setting and the children in your care from accidental damage and online criminals via National Cyber Security Centre

Useful resources and websites

1. Data Protection Act and Freedom of Information Act. Available to download from http://www.legislation.gov.uk/
2. Data Protection via LBWF Hub https://thehub-beta.walthamforest.gov.uk/data-protection
3. National Cyber Security Centre
4. Nursery Cyber Security by NDNA
5. Information Commission Office (ICO) UK GDPR guidance and resources
6. DfE Information Sharing: Guidance for practitioners and managers ref DCSF-00807-2008 https://www.gov.uk/government/organisations/department-for-education
7. Providers must be aware of their responsibilities under the, Data Protection Act 2018. If they are a public body, the Freedom of Information Act 2000 applies.
8. Data protection rules for businesses in recruiting staff, keeping staff records and using CCTV: Data protection and your business
9. Record retention advice from CIPD
10. LBWF Early Years & Childcare Privacy Notice Template
11. Data Protection Act and Freedom of Information Act. Available to download from http://www.legislation.gov.uk/

12. Data Protection tips for Early Years settings by ICO