Information Management Toolkit
Early Years Provision
Version April 2019

Disclaimer:

This toolkit has been created to advise those setting involved with early years provision about records management and record retention. The information contained in this document for general information purposes only. While every effort has been made to keep the information up to date and correct, Kent County Council makes no representations or warranties of any kind, expressed or implied, about the completeness, accuracy, reliability of suitability with respect to the information containined within this guidance. Any reliance placed on such information is therefore strictly at the user's risk.

Contents

Introduction

This toolkit has been created for the use of early years providers. It is intended to be a framework against which settings can create their own records management programme. As settings are usually run as businesses or as a charitable trust or in some cases by sole traders, the legislative framework may be different. So that this toolkit is as easy to use as possible, generic advice is provided in some cases, where appropriate a note is included which refers the setting to business rules or the provisions of the Charity Commission. It is the responsibility of the setting owner or the charitable trustees to ensure that their information management framework is compliant with the requirements of their sector.

The retention periods shown below can only be guidance and it is up to each individual setting whether they implement the retention periods shown below after having undertaken a business risk analysis.

Maintaining and storing the records relating to their setting is the responsibility of the individual setting owner or charitable trustees [see below about what to do if a setting or charitable trust is sold or needs to be closed down].

Freedom of Information Act 2000

Unless the setting is wholly or partly owned by a public authority then it is not subject to the requirements of the Freedom of Information Act 2000.

Data Protection Act 2018 and General Data Protection Regulations 2016

All settings are subject to the requirements of the Data Protection Act 2018 and the General Data Protection Regulations 2016. There are a number of checklists created by the Information Commissioner's Office which will allow settings to assess their compliance with this legislation.

The checklist for small businesses and sole traders can be found at:
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/assessment-for-small-business-owners-and-sole-traders/

The checklist and other resources for charitable trusts can be found at:
https://ico.org.uk/for-organisations/charity/

From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 requires every organisation or sole trader who processes personal information to pay a data protection fee to the ICO, unless they are exempt. For more information about this, please visit https://ico.org.uk/for-organisations/data-protection-fee/.

Unless a setting is part of a bigger organization or part of a public authority, they will not need to appoint a Data Protection Officer or to complete the Article 30 Record of Processing Activity (ROPA).

All settings will need to ensure that they have created a privacy notice.

For more information about implementing the Data Protection Act 2018 and the General Data Protection Regulations 2016 please visit
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Records Storage – Physical

Physical records must be managed to ensure that they cannot be lost, damaged or destroyed. Settings must also ensure that records are protected from unauthorised access or theft. Records containing personal data must be stored in locked filing drawers and where possible in an area which is supervised. Records should not be stored in an area which is accessed by other organizations or users unless there is no alternative even if the cabinets or filing drawers are locked.

Checklist 1, which can be found at the end of this toolkit, has been extracted from KCC's information management manual, and provides some basic guidance about the standards around records storage.

Records Storage – Electronic

Electronic records must be managed to ensure that they cannot be lost, damaged or destroyed. Settings must also ensure that records are protected from unauthorised access or theft. Records containing personal data must be password protected or encrypted[1]. Electronic records should be backed up regularly and where possible the back-up should be stored away from the main device.

Where records are stored on portable storage media, such as flash drives or portable hard drives, the devices should be password protected or encrypted. The devices should be backed up on a regular basis and where the data is not in regular use should be checked to make sure that it is still readable on a routine basis.

It is strongly recommended that settings do not store personal information in cloud based solutions unless there is no other alternative. If the storage is located in the USA or other non-EU areas then the setting will not be compliant with the General Data Protection Regulations 2016. However, cloud storage could be suitable for the storage of business records.

[1] If records are encrypted it is important to retain a safe copy of the encryption key.

Disposal of Records

Records should be disposed of on a routine basis using the retention schedule as guidance. Best practice states that a record is kept of disposals which are made although this is not a legal requirement.

Physical records should be disposed of in a way that ensures that personal information is not compromised. All records containing personal information should be shredded before disposal.

Digital records

Digital records must be disposed of with care. It is possible to retrieve data that you think has been deleted from magnetic media using specialist software that is readily available.

Remember, deleted documents remain stored in the Recycle Bin until it is emptied. This is to ensure that documents are not deleted by mistake. You must empty your recycle bin on a regular basis to ensure that the documents have been deleted from the device.

Data on the hard drive of a laptop or desktop computer is unlikely to be overwritten immediately which means that the data could be retrieved from the the hard drive using data recovery software

Records can be deleted from flash drives and external hard drives using the standard document deletion process. Some external devices and external hard drives do have a recycle bin facility, if this is the case you must ensure that the recycle bin is emptied.

You should reformat the device periodically, especially if you have used the device for transporting information rather than storage, to ensure that any imprint the document has left on the device has been removed.

If you are planning to sell on device then the hard drive must be re-formatted.

Sample Disposal Schedule

The following records were destroyed according to the retention period laid down in the early year provider's retention schedule or on the authorisation of the officer named below*

*delete as appropriate

File Reference	Brief description	On whose authority	Method of disposal

Information Sharing

It is likely that settings will need to share information with other organizations and individuals. Settings should be clear about what information they hold and with whom it can be shared.

Other than when sharing information as part of a statutory requirement, you will require the consent of the individual concerned and in the case of sensitive personal data explicit consent of the data subject (or the individual with parental responsibility if it is a child's data). All this information should be included in a privacy notice.

All requests for access to personal information should be deal with in line with the requirements laid down in the Data Protection Act 2018 and The General Data Protection Regulations 2016.

When a Setting Closes

There may be a number of reasons why a setting closes:

1. If the business is sold then it is the responsibility of the seller to ensure that business records are maintained in line with legal requirements. The seller will remain responsible for the children's records (other than those who are continuing to attend the setting) unless the new owner is prepared to take responsibility for historical records (usually there would be a provision in the contract)

2. If the setting closes but the business is not being sold on (i.e. the owner is retiring or has died), then it is the responsibility of the owner or their executors to ensure that business records are maintained in line with legal requirements. The owner or their executors will remain responsible for the children's records.

3. If the setting closes because the business has gone into administration, then the business and records will become the responsibility of the administrators.

4. If a setting which is run as a charitable trust closes, then the records must be managed in line with the Charity Commission's requirements.

It is recommended that the setting contact their legl advice line through their insurance, and to seek advice from the Information Commissioners Office (www.ico.org.uk).

Records, especially those containing personal information, should not be abandoned in the building when a setting is closed. This will constitute an information security under the General Data Protection Regulations 2016 and the Data Protection Act 2018.

Retention Guidelines

The retention periods listed below are only guidelines, where appropriate settings should undertake information risk analysis to identify retention periods or seek legal advice. The responsibility with developing and implementing records retention rests with the individual setting.

The retention periods listed below are not intended to be exhaustive.

For further information about retention please see:

The Information Management Toolkit for Schools (https://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/records-management)

The Kent County Council Retention Schedule (https://www.kent.gov.uk/about-the-council/contact-us/access-to-information)

For further advice about retention periods please contact the KCC Records Manager, Elizabeth Barber (03000 415812) or elizabeth.barber@kent.gov.uk.

Identifier	Description	Retention Period	Authority	Disposal
EYPS1	**Children's Records**			
EYPS1.1	Records relating to individual children attending the setting which are not passed onto the primary school when the child transfers	DOB + 25 years	Limitation Act 1980 (Section 2)	SECURE DISPOSAL
EYPS1.2	All records relating to child protection including referrals to and contact with social services including the Local Authority Designated Officer	These records should not be disposed of until the Independent Inquiry Into Child Sexual Abuse (IICSA) have completed their report and made their recommendations		SECURE DISPOSAL
EYPS1.3	Registers of attendance	Date of last Ofsted inspection + 3 years [The framework states that the records should be kept for a "reasonable" period of time]	Early Years Foundation Stage Welfare Requirements	SECURE DISPOSAL
EYPS1.4	Records of medication administered to the children	Date of birth + 22 years	Limitation Act 1980 (Section 11)	SECURE DISPOSAL
EYPS2	**Health and Safety**			
EYPS2.1	Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Date of the accident + 4 years or date any insurance claim or compensation payment is made + 6 years which ever is the longer	Limitation Act 1980 (Section 11)	SECURE DISPOSAL
EYPS2.2	Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Date of birth + 22 years or date any insurance claim or compensation payment is made + 6 years which ever is the longer	Limitation Act 1980 (Section 11)	SECURE DISPOSAL

Identifier	Description	Retention Period	Authority	Disposal
EYPS2.3	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR) For more information see http://www.hse.gov.uk/RIDDOR/	Records should be kept for a minimum of 3 years from the date of the incident	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013	SECURE DISPOSAL
EYPS2.4	Records relating to incidents specified by the Control of Substances Hazardous to Health Regulations (COSHH) 1999 For incidents concerning asbestos or radiation please seek the assistance of the Health and Safety Executive	Date of incident + 40 years	Control of Substances Hazardous to Health Regulations (COSHH) 1999/2002	SECURE DISPOSAL
EYPS3	**Personnel Records**			
EYPS3.1	Personnel records relating to individual members of staff	Date of termination of employment + 6 years	Chartered Institute of Personnel and Development	SECURE DISPOSAL
EYPS3.2	Allegation against anyone involved within the child care organisation (paid or unpaid) A copy should be given to the individual and a copy should be	Retained on file for all staff who have been subject to an allegation (regardless of whether they are still employed in the setting) until the person reaches the normal retirement age or for 10 years from the date of the allegation whichever is the longer	Children Act 1989/2004	SECURE DISPOSAL

Identifier	Description	Retention Period	Authority	Disposal
	stored in the individual's confidential file)[2]			
EYPS3.3	Application forms and interview notes (for unsuccessful candidates)	6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months.	Chartered Institute of Personnel and Development	SECURE DISPOSAL
EYPS3.4	Disclosure and Barring Check [This includes everyone working, volunteering – including management committees, and people living on the premises within the childcare organisation]	Date employment ceases + 6 years Do not keep the disclosure document, make note of 5 relevant pieces of information[3]	Disclosure and Barring Service Code of Practice	SECURE DISPOSAL
EYPS3.5	Complaints Record Book	Date of the last record + a minimum of 3 years or until next Ofsted inspection whichever is the longer	Early Years Foundation Stage Welfare Requirements	SECURE DISPOSAL
EYPS4 Payroll Records				
All information relating to the management of payroll records can be found on the web page https://www.gov.uk/paye-for-employers/keeping-records				

[2] Guidelines set by the Local Safeguarding Children's Board: Records of the allegation must be clear and comprehensive, detailing: Any allegations made; Details of how allegations were followed up and resolved; Any action taken; Decisions reached

[3] DBS Code of Practice: Retain the following after the certificate is destroyed – 1. The date of issue of a disclosure; 2. The name of the subject; 3. The type of the disclosure requested; the position for which the Disclosure was requested; 4. The unique reference number of the Disclosure; 5. The details of the recruitment decision taken.

Identifier	Description	Retention Period	Authority	Disposal
EYPS5	**Finance and Accounting Records**			
Retention periods for Finance and Accounting records will differ depending on the type of business, company or charitable trust.				
EYPS5.1	Finance and accounting records created by a limited company	https://www.gov.uk/running-a-limited-company/company-and-accounting-records		SECURE DISPOSAL
EYPS5.2	Finance and accounting records created by a sole trader	https://www.gov.uk/self-employed-records		SECURE DISPOSAL
EYPS5.3	Finance and accounting records created by charitable trusts	https://www.gov.uk/government/publications/charity-reporting-and-accounting-the-essentials-cc15b/charity-reporting-and-accounting-the-essentials		SECURE DISPOSAL
EYPS5.4	For all records relating to the completion of tax returns	https://www.gov.uk/hmrc-internal-manuals/compliance-handbook/ch10000		SECURE DISPOSAL

Settings should retain administration records in line with the requirements of the type of business or charitable trust.

Checklist 1: Physical Storage Requirements

Standard Recommendations (We recognise that some provider types may not feel able to meet these recommendations in their entirety):

The buildings/rooms chosen for records storage should be entirely weatherproof.

It is not appropriate to store records in buildings such as barns, sheds or garages where water gets into the buildings. It is also not appropriate to store records in a room where the roof leaks into the room.

The buildings/rooms chosen for records storage should be in a location which is free from the threat of arson or other acts of vandalism.

It is not appropriate to use buildings which are located in areas which have a high crime or vandalism rate. Arson is a real threat to records stored in buildings in this kind of area.

The buildings/rooms chosen for records storage should be secured against unauthorised access and should have the appropriate security measures in place.

The buildings/rooms chosen for records storage should have adequate fire detection apparatus.

At a minimum this should include heat/smoke detection equipment. Fire is a real threat to paper storage areas as paper is combustible.

The buildings/rooms chosen for records storage should have a free circulation of air around the room.

This will prevent the formation of mould in the room.

Records should not be stored on the floor in case of flood.

Records should be stored at least 2" off the ground. Where possible records should be stored in cupboards, cabinets and drawers to protect from water or fire damage.

Requirements for storage used solely for records storage

The buildings/rooms chosen for records storage should be used solely for records storage where possible.

Records should not be stored in rooms which are used as “dumping grounds” for old equipment or other detritus (e.g. Christmas decorations). Cleaning materials, especially inflammable liquids, must not be stored in the same storage areas as records.

The buildings/rooms chosen for records storage should be kept to a stable temperature of between 15ºC and 27ºC and a relative humidity of between 30% and 60%.

The temperature and relative humidity should be stable within these bands. Violent fluctuations of temperature can cause conditions which encourage the growth of mould.

The buildings/rooms chosen for records storage should be free from insect or rodent infestation.

Records should not be stored in rooms which have a systemic problem either with insect or rodent infestation.

The buildings/rooms chosen for records storage should be checked regularly for degradation in environmental conditions and possible insect/rodent infestation.

This may involve using technical equipment to record temperature and humidity but it may be as simple as a weekly inspection to ensure that there is no mould growth and that there is no evidence of insect/rodent infestation. The record rooms must be kept tidy and free from rubbish and boxes should not cause a trip hazard or block exits and entrances to the room.

Records stored in these buildings/rooms should be boxed and listed in a way that will allow easy retrieval when it is required.

Boxes provide a measure of protection from all the environmental hazards identified above (i.e. fire, flood, insect/rodent damage) and also offer a first line barrier against unauthorised access to the records. If the records are not listed in a way which means that they can be located and retrieved easily then there is little point in storing the records in the first place. The records storage area will rapidly become a dumping ground for records which are not being managed properly. It is strongly recommended that employees do not put a list of the contents of the box on the box label, especially if the records contain personal information. A box reference number should be sufficient but if necessary a brief description of the record series can be included on the outside of the box.

Boxes stored in the record room should be placed on shelves where possible.

Shelves allow for easy access to the boxes and ensure that the area is managed in a systematic way. The bottom shelf should always be at least 2” from the ground (this is a basic precautionary measure to limit water damage if an area is flooded). If shelving is not used then boxes of records must be stored on pallets. The top of the pallet must be raised at least 2” from the ground (this is a basic precautionary measure to limit water damage if an area is flooded). If the pallet has more than 6 layers of boxes then the pallet should be shrink wrapped.