Retention and Destruction of Records Guidance

Disclaimer:

*Retention periods are either stipulated in legislation or ‘best practice’ for example H.M Customs will have specific requirements in relation to financial records. This guidance is intended to support Settings/ Childminder’s in considering the types of records that should be kept after a child has left and the length of time that they should be kept securely for. For example, records such as accident and child protection records*.

|  |
| --- |
| **Legal, Statutory and Supporting Guidance** |
| **The Early Years Statutory Framework (EYFS, 2021)**  The period for which records need to be retained maybe influenced by the following legislation and general good practice. The Early Years Statutory Framework (EYFS, 2021) states:  3.69. Providers must maintain records and obtain and share information (with parents and carers, other professionals working with the child, the police, social services and Ofsted or the childminder agency with which they are registered, as appropriate) to ensure the safe and efficient management of the setting, and to help ensure the needs of all children are met ***65***. Providers must enable a regular two-way flow of information with parents and/or carers, and between providers, if a child is attending more than one setting. If requested, providers should incorporate parents’ and/or carers’ comments into children’s records.  3.70. Records must be easily accessible and available (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 ***66***. Providers must be aware of their responsibilities under the Data Protection Legislation ***67*** and where relevant the Freedom of Information Act 2000.  3.71. Providers must ensure that all staff understand the need to protect the privacy of the children in their care as well the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality. Parents and/or carers must be given access to all records about their child, provided that no relevant exemptions apply to their disclosure under the Data Protection Act ***68***.  3.72. Records relating to individual children must be retained for a reasonable period of time after they have left the provision ***69***.  ***65*** Guidance on sharing information with relevant services when there are safeguarding concerns is available via: <https://www.gov.uk/government/publications/safeguarding-practitioners-informationsharing-advice>  ***66*** The National Cyber Security Centre (NCSC) has published helpful guidance on cyber security:  <https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings>  ***67*** This includes the Data Protection Act 2018 and General Data Protection Regulation 2018 see: <https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>  ***68*** The Data Protection Act 2018 (DPA) gives parents and carers the right to access information about their child that a provider holds. However, the DPA also sets out specific exemptions under which certain personal information may, under specific circumstances, be withheld from release. For example, a relevant professional will need to give careful consideration as to whether the disclosure of certain information about a child could cause harm either to the child or any other individual. It is therefore essential that all providers/staff in early years settings have an understanding of how data protection laws operate. Further guidance can be found on the website of the Information Commissioner’s Office at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>  ***69*** Individual providers should determine how long to retain records relating to individual children. |
| **Safeguarding – Working Together to Safeguarding Children (2018)** |
| Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, as provided for in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).  To share information effectively: • all practitioners should be confident of the processing conditions under the Data Protection Act 2018 and the GDPR which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as ‘special category personal data’ • where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 contains the Data Protection Act 2018 contains ‘safeguarding of children and individuals at risk’ as a processing condition that allows practitioners to share information, including without consent (where in the circumstances consent cannot be given, it cannot be reasonably expected that a practitioner obtains consent or if to gain consent would place a child at risk. ( Point 28 page 20 ) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729914/Working_Together_to_Safeguard_Children-2018.pdf> |
| **Information Commissioners Office (ICO)** |
| * How Personal data will be processed and for what purposes. * How long personal data will be kept for and the decisions for retaining some records. * How records will be securely deleted when records are no longer required. * How records will be updated, archived or securely deleted.   The GDPR sets out seven key principles:   * + Lawfulness, fairness and transparency   + Purpose limitation   + Data minimisation   + Accuracy   + Storage limitation   + Integrity and confidentiality (security)   + Accountability   These principles should lie at the heart of your approach to processing personal data.  For further information:  <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/>  <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>  The ICO offers a useful guide on the principles to consider when making decisions about the retention and destruction of records.  <https://ico.org.uk/for-organisations/guide-to-data-protection/>  The Data Protection Act which includes GDPR does not set out any specific minimum or maximum periods for retaining personal data. |
| **Insurance Company** |
| Settings should confirm with their Insurance Company the timescales they are required to keep particular records for. For example, the Insurance Company may require Accident Records to be retained for a specific period of time. |
| **Membership Guidance e.g. PLA Pre School Leaning Alliance, PACEY** |
| It’s important that settings seek advice from their own Membership Organisations as appropriate, as they may have supporting guidance. |
| **Other guidance that needs to be taken into account includes:** |
| Health and Safety requirements, H.M. Customs and Excise requirements, Inland Revenue requirements, Grant claim requirements (e.g. Early Education Funding, Grants Awarded). |
| **What types of personal records do we hold?** |
| * Consider the types of records held * Paper * Electronic files (including database, Word documents, PowerPoint presentations, Spreadsheets, webpages and e-mails) * Photographs, scanned images, CD-ROMs and video tapes * Minutes of meetings * Submissions from external parties * Contracts and invoices * Registers * Childrens records * Safeguarding records * Legal advice * File notes * Funding paper work and data * Financial accounts * Employee information (prospective, existing and former) * Information shared with software providers (e.g. electronic learning journal) * Display boards |
| **Why retain records and documentation?** |
| It may be necessary to retain some records relating to a child or family after they have left the setting. The timescales will depend on the types of records and the nature of their content. |
| **The settings policy should also include:** |
| * The management and control of personal data is defined as any information relating to an identified or identifiable individual. This includes being able to identify a person directly or indirectly. * The responsibility which shows who made the decision and the basis it was made. This is especially relevant for day care providers for 'historical queries' where you can no longer ask the individual concerned (e.g. the actions of an employee who has since left the setting). * The authority to show that the person who made the decision had the appropriate delegation and seniority to do so. * The accountability to enable those involved in the decisions of the retention and destruction of records, including financial records to show they have acted honestly and in accordance with the settings policy. To demonstrate to outside organisations (as appropriate) that the setting can account for all decisions made or how for example the money was spent. * The judgments made about the current and future value of the information in line with the purpose for which it was obtained and its nature. |
| **Storage of Records and Confidentiality** |
| * Care should be taken to ensure records are kept in an appropriate location. * Where access restrictions are appropriate to sensitive documents, secure storage measures should be in place e.g. locked filing cabinets, password protected files if held electronically. * In an environment that will not cause the records to deteriorate quickly e.g; damp, records kept on discs should not be exposed to heat etc. * In a location where they do not constitute a Health and Safety risk. * Folders or containers should be clearly labelled to show the records they contain to minimise delays in retrieval and display a clearly marked disposal /destruction date. |
| **Sharing of Data** |
| By law we must share information when a child is at risk of harm. However, knowing whether to share and what to share can sometimes be worrying, even when the law tells us we must. These worries are particularly likely to appear when engaging in preventative work or intervening early to stop concerns escalating. Statutory guidance identifies seven golden rules set out by central government to make things clearer for everyone (Coventry Safeguarding Children Partnership CSCP). |
| **Seven Golden Rules for Sharing Information** |
| 1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately. 2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so. 3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible. 4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case. 5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions. 6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely. 7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.   (Reference: Seven golden rules for information sharing, Coventry Safeguarding Children Partnership (CSCP)  **For more detailed information please visit:**  **Seven Golden Rules Information Sharing Poster**  <http://www.coventry.gov.uk/downloads/file/22957/information_sharing_poster> |
| **Information Sharing -**  Advice for practitioners providing safeguarding services to children,  young people, parents and carers **(July 2018)** |
| This HM Government advice is non-statutory and has been produced to support practitioners in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being.  <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf> |
| **Disposal of records** |
| * Once records have been retained for the appropriate period they may be disposed of (this is particularly valid to 'personal' information relating to individuals where there is a duty to dispose of the records after a specified period). * Care should be taken to ensure information is destroyed securely - e.g; shredding sensitive paper records and establishing protocols for erasing electronic records. * A schedule should be created to demonstrate when records have been destroyed/deleted. |
| **Guide to Retention Periods for Records** |
| A judgement must be made about:   * The current and future value of the information. * How long you should keep personal data depends on the purpose for which it was obtained and its nature. * Where personal data is held for more than one purpose, there is no need to delete the data while it is still needed for any of those purposes. However, personal data should not be kept indefinitely “just in case”, or if there is only a small possibility that it will be used. |
| **Retention and Destruction of Records Guidance** |
| PACEY - <https://www.pacey.org.uk/Pacey/media/Website-files/PACEY%20member%20practice%20guides%20(PDFs)/PACEY%20member%20practice%20guides%202017%20(PDFs)/PG27-Record-keeping.pdf>  NSPCC - <https://learning.nspcc.org.uk/research-resources/briefings/child-protection-records-retention-storage-guidance> |