BASE CAMP AT BALDERSBY PARK

# Data Protection Policy

Last updated May 2026 · Review due May 2027

## Guiding principles of records management

According to Data Protection principles, records containing personal information should be:

- adequate, relevant and not excessive for the purpose(s) for which they are held
- accurate and up to date
- only kept for as long as is necessary (Information Commissioner's Office, 2021).

The introduction of the General Data Protection Regulation (GDPR) in 2018 does not change the way child protection records should be stored and retained.

Base Camp will ensure staff:

- know the reason why we're keeping records about children and/or adults (for example, because they relate to child protection concerns)
- assess how long we need to keep the records for
- have a plan for how and when the records will be destroyed.

To keep personal information secure, we will:

- compile and label files carefully
- keep files containing sensitive or confidential data secure, and allow access on a 'need to know' basis.

If we are creating records about the children and/or adults that take part in our services or activities, we should make sure they understand what records we hold (see Privacy Policy), why we need to hold them, and who we might share their information with (for example, as part of a multi-agency child protection team). If we are keeping records for child protection reasons, we don't necessarily need to get consent from the adults and/or children concerned.

## Concerns about children's safety and wellbeing

If Base Camp has concerns about a child or young person's welfare or safety, it's vital all relevant details are recorded. This should be done regardless of whether the concerns are shared with the police or children's social care.

Base Camp will keep an accurate record of:

- the date and time of the incident/disclosure
- the date and time of the report
- the name and role of the person to whom the concern was originally reported, and their contact details

- the name and role of the person making the report (if this is different to the above), and their contact details
- the names of all parties who were involved in the incident, including any witnesses
- the name, age and any other relevant information about the child who is the subject of the concern (including information about their parents or carers and any siblings), and what was said or done and by whom
- any action taken to look into the matter
- any further action taken (such as a referral being made)
- the reasons why the organisation decided not to refer those concerns to a statutory agency (if relevant).

## Information sharing

When sharing information with any organisation, Base Camp will consider the DfE guidance "Information sharing advice for safeguarding practitioners", which describes key principles for deciding what to share. The seven golden rules for information sharing are:

1. Remember that the Data Protection Act and GDPR legislation are not a barrier to sharing information — the welfare of the child is the paramount concern. As long as the information can be justified and is in accordance with this information sharing guidance, it should be shared.
2. Be open and honest — where appropriate, it is important to keep all parties informed of information sharing plans, processes and boundaries.
3. Seek advice — from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with consent where appropriate — consent of the individual concerned should be sought before sharing. However, consent may not be appropriate if informing the individual would place a child at risk, or you can dispense with consent if sharing information is in the best interests of the child.
5. Consider safety and well-being — include considerations of support needs for all involved, including those about whom information is being shared, any risks of sharing the information and how these would be managed.
6. Keep a record — recording is important at every stage, including recording how and why decisions were made about information sharing. All records should be signed and dated.
7. Necessary, proportionate, relevant, accurate, timely and secure — the key one:
    - **Necessary** — is the information necessary to keeping the child or children safe?
    - **Proportionate** — how much information needs to be shared? It may not be appropriate to share all information.
    - **Relevant** — only include information that is relevant to the situation and required to make decisions or take action to keep children safe. Only share information with relevant people; confidentiality of personal and case information should be upheld.

- **Accurate** — include factual information. If any opinions are stated, these should be evidence-based. Include times and dates of information and accurate information about individuals concerned.
- **Timely** — share information at the earliest opportunity; avoid delay. However, don't rush into sharing information without the appropriate decision-making processes.
- **Secure** — how is information shared, stored, and for how long?

## Conclusion

Compliance with the Data Protection Act 2018 is the responsibility of all members of staff and contractors. Any questions about this policy, or any queries concerning data protection matters, should be raised with Hannah Secouet.

## Definitions

**Subject Access Request (SAR)** — A request for access to data by a living person under the Act. All records that contain the personal data of the subject will be made available, subject to certain exemptions.

**Freedom of Information Request (FOI)** — A request for access to data held, dealt with under the Freedom of Information Act 2000. Requests for the data of deceased people may be processed under this legislation.

**Personal data** — Data which relate to a living individual who can be identified directly or indirectly from the data, particularly by reference to an identifier. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). Examples include the name and address of an individual, email and phone number, a Unique Pupil Number or an NHS number.

**Special category data** — Certain personal data given special protections under the Act, because misuse could create more significant risks to a person's fundamental rights and freedoms (for example, by putting them at risk of unlawful discrimination). Information relating to criminal activities or convictions is not special category data, but must be treated with similar safeguards in place. Special category data includes:

- race or ethnic origin of the data subject
- their political opinions
- their religious beliefs or other beliefs of a similar nature
- whether they are a member of a trade union
- their physical or mental health or condition
- their sexual life
- sexual orientation
- biometrics (where used for ID purposes)
- genetics.

**Confidential data** — Data given in confidence, or data which is confidential in nature and that is not in the public domain. Some confidential data will also be personal data and/or special category data, and therefore come within the terms of this policy.

**Data controller** — The organisation which determines the purposes, and the way, any personal data is processed. Base Camp is the data controller of all personal data used and held.

**Data processors** — Organisations or individuals who process personal data on behalf of the data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

**Data subject** — A living individual who is the subject of personal data. This need not be a UK national or resident; rights with regard to personal data are available to every data subject, wherever their nationality or residence.

**Lawful basis** — The grounds specified by the Regulations which need to be satisfied for any data processing to be legal. One ground needs to exist for processing personal data. Where special category data is processed, a second ground must also exist.

**Data breach** — A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A data breach may occur by accidentally sending an email to the wrong person, or leaving a file in a public place. Breaches which result in a high risk to the individual must be reported to the ICO within 72 hours.

NSPCC guidelines surrounding retention and destruction of personal information will be strictly followed. More information can be found in the NSPCC's child protection records retention and storage guidelines.