

ACTIVITIES 4 KIDS: GDPR & DATA PROTECTION POLICY



OCTOBER 2026

Briony Jacobs & Daisy Jacobs-Milburn

ACTIVITIES 4 KIDS | 215 ELM DRIVE, HOVE, BN3 7JD



GDPR & DATA PROTECTION POLICY

Activities 4 Kids — Ofsted-registered children's holiday camp

Policy owner	Activities 4 Kids Management / designated data protection contact
Policy date	15 October 2026
Next review	15 October 2027, or sooner if law, guidance or processing changes
Applies to	Staff, volunteers, contractors, agency workers and anyone handling personal data for Activities 4 Kids

Important: This is an operational policy draft. Activities 4 Kids must confirm its actual data flows, software providers, retention periods, privacy notices, contact details and whether it is required to appoint a Data Protection Officer (DPO). A policy alone does not establish compliance.

1. Purpose and commitment

Activities 4 Kids respects the privacy of children, parents and carers, employees, applicants, volunteers, contractors and other people whose personal information it handles. We will use personal data lawfully, fairly and transparently, collect only what we need, keep it accurate and secure, and retain it only for as long as necessary or legally required.

Children's information requires particular care. Decisions about children's data will take account of their best interests, age, understanding and safeguarding needs. This policy is intended to support compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended, and other applicable law and guidance.

2. Scope

This policy applies to all personal data handled by Activities 4 Kids in paper, electronic, photographic, video, audio or other formats. It covers information gathered during enquiries, bookings, attendance, activities, safeguarding, staff recruitment and employment, payments, communications, marketing and service administration.

All staff and other people acting on behalf of Activities 4 Kids must follow this policy and any related privacy notices, retention schedule, information-security procedures, safeguarding policy and incident-reporting process.

3. Key terms

- **Personal data:** information relating to an identified or identifiable living person.
- **Special category data:** particularly sensitive information, such as health information, where additional legal conditions apply.
- **Processing:** collecting, viewing, using, storing, sharing, changing or deleting personal data.
- **Data breach:** a security incident leading to accidental or unlawful loss, alteration, destruction, disclosure of or access to personal data.
- **Data subject:** the person the information is about.



4. Roles and responsibilities

- Activities 4 Kids Management is responsible for ensuring appropriate policies, systems, training and resources are in place and for deciding how and why personal data is processed.
- The designated data protection contact will coordinate privacy requests, record incidents, maintain the data inventory and retention schedule, support risk assessments and seek specialist advice when needed. This contact is not automatically a statutory DPO.
- All staff, volunteers and contractors must access information only where authorised, use approved systems, maintain confidentiality, complete training and report suspected incidents immediately.
- Third-party providers must be assessed and given appropriate written instructions and contractual protections where they process data on Activities 4 Kids' behalf.

5. What information we may collect

Depending on the service and role, Activities 4 Kids may process:

- Children's names, dates of birth, age, attendance, booking details and emergency contacts.
- Parent/carer names, contact details, collection permissions and relevant parental responsibility or court-order information where needed for child safety.
- Relevant medical, allergy, dietary, disability, additional-needs and medication information needed to care for a child safely.
- Safeguarding, accident, incident, behaviour and concern records where necessary for child welfare and legal duties.
- Photographs, video or audio recordings, where there is a defined purpose and appropriate authority, notice and permissions.
- Payment, invoice and transaction details; we should not retain full payment-card details unless there is a lawful and secure reason.
- Staff, applicant and volunteer information, including identity, right-to-work, qualifications, references, training and DBS information where lawful and relevant.
- Website enquiry, email and communication records, and technical information generated by systems used to run the service.

We will not collect information simply because it might be useful in future. Access to sensitive information will be limited to people who need it for their role.

6. Lawful, fair and transparent use

Before processing personal data, Activities 4 Kids will identify and document an appropriate lawful basis under the UK GDPR. Depending on the purpose, this may include performance of a contract, compliance with a legal obligation, legitimate interests, vital interests or consent. Special category data requires an additional applicable condition. Consent will not be used as a blanket basis for all processing.

Privacy notices will explain who is responsible for the information, what is collected, why it is used, the relevant lawful basis, who receives it, retention periods or criteria, individuals' rights and how to complain to the Information Commissioner's Office (ICO). Notices for children will be clear, accessible and age-appropriate, with information also made available to parents/carers as appropriate. <Cite refs=[['turn674984search0', 'turn674984search2']]>



We will use personal data only for specified, explicit and legitimate purposes. If a new purpose is proposed, management will check whether it is compatible with the original purpose or whether further notice, a new lawful basis or consent is required.

7. Children's information, health and safeguarding records

- Collect only the health and care information reasonably needed to keep children safe and deliver the service.
- Make sensitive information available only to staff who need it to support the child, respond to an emergency or meet a legal/safeguarding responsibility.
- Do not discuss a child's information where other parents, children or unauthorised people can overhear.
- Share information with children's social care, police, Ofsted or other relevant authorities where lawful and necessary to safeguard a child or comply with legal duties. Do not delay an urgent safeguarding referral solely because parental consent has not been obtained.
- Keep safeguarding and incident records factual, proportionate, dated and securely stored. Do not promise absolute confidentiality where information may need to be shared to protect a child.
- Where a child or parent exercises data rights, consider the child's own capacity and best interests and any safeguarding risks before responding to a parent's request for the child's information.

Activities 4 Kids will assess whether a Data Protection Impact Assessment (DPIA) is required for processing likely to create a high risk to people's rights and freedoms, and will consider the heightened risks involved in sharing children's data. <Cite refs=[['turn674984search4','turn674984search5']]/>

8. Photographs, video and communications

- Use images only for a clear, stated purpose and follow the separate photo/video consent or permissions process where applicable.
- Explain whether images will be used for internal records, parent updates, publicity, social media or other purposes; do not treat permission for one purpose as permission for every purpose.
- Respect objections and withdrawals of consent where consent is the lawful basis, and explain any limits where an image has already been published or is held for another lawful reason.
- Use approved devices and accounts. Staff must not store children's images on personal devices or share them through personal messaging or social-media accounts unless expressly authorised under a documented, secure procedure.
- Check recipients and attachments before sending messages. Use suitable recipient controls, such as BCC where appropriate, to avoid disclosing families' contact details to one another.

9. Accuracy, minimisation and retention

We will take reasonable steps to keep personal data accurate and up to date, correct inaccuracies promptly and collect only what is relevant and necessary. Activities 4 Kids will maintain a retention schedule identifying the type of record, purpose, retention period or criteria, and secure disposal method. Different records have different retention requirements; there is no single retention period for all records.

When information is no longer needed, it will be securely deleted, shredded or anonymised, unless it must be retained for a legal obligation, safeguarding matter, dispute, insurance claim or other lawful reason. Any retention exception must be documented and reviewed.



10. Storage and security

- Use strong, unique passwords and multi-factor authentication where available; never share logins.
- Keep paper records in locked storage and electronic records in access-controlled systems.
- Limit access by role and remove access promptly when a person leaves or changes duties.
- Use approved, updated devices and software, screen locks, encryption and secure backups where available.
- Do not send personal data to personal email accounts, unapproved cloud storage or removable media.
- Check the identity and authority of anyone requesting information, particularly by phone or email.
- Use secure disposal methods for paper and electronic records and ensure equipment is wiped securely before disposal or reuse.
- Report phishing, malware, lost devices, misdirected emails, unauthorised access and other security concerns immediately.

11. Sharing data and suppliers

Activities 4 Kids will share personal data only where there is a lawful, necessary and proportionate reason. This may include staff who need the information, parents/carers where appropriate, payment or booking providers, insurers, professional advisers, emergency services, children's social care, police, Ofsted or other regulators. Sharing children's data requires particular care and should take account of the child's best interests. <Cite refs=[['turn674984search4']]>/>

Before using a supplier that processes personal data on our behalf, management will carry out proportionate checks and put in place a written data-processing agreement where required. The agreement should cover documented instructions, confidentiality, security, sub-processors, assistance with rights requests and breaches, deletion/return of data and audit or compliance information. International transfers must be checked and protected using a lawful transfer mechanism where required.

12. Individual rights and requests

People have rights under data-protection law, subject to legal conditions and exemptions. These may include the right to be informed, access their data, correct inaccurate data, request erasure, restrict processing, object, and receive or transfer certain data. Not every right applies in every circumstance.

1. Any request should be sent promptly to the designated data protection contact and logged with the date received.
2. Verify the requester's identity and authority proportionately. For a request about a child, consider the child's capacity, best interests and safeguarding circumstances.
3. Search relevant systems and paper records, consult appropriate staff and assess applicable exemptions, third-party information and safeguarding risks.
4. Respond without undue delay and normally within one month. If the request is complex or multiple requests are received, a lawful extension may be available; tell the requester within the initial month and explain why.
5. Do not delete or alter relevant information simply because a request has been made. Seek advice if a request involves safeguarding, litigation or a potential exemption.

Individuals may also complain to the ICO. Activities 4 Kids will cooperate with the ICO and respond to enquiries appropriately.



13. Personal data breaches

A suspected breach must be reported to management or the designated data protection contact immediately, even if it seems minor. Examples include an email sent to the wrong recipient, a lost phone or paper file, a compromised account, unauthorised access, or records disclosed without permission.

6. Contain the incident where possible without destroying evidence. For example, recall a message if available, ask an unintended recipient to delete it and not share it, or disable a compromised account.
7. Record what happened, when it was discovered, what data and people may be affected, likely consequences and steps taken.
8. Assess the risk to people's rights and freedoms, with particular attention to risks for children and sensitive information.
9. Where required, notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to individuals, inform affected people without undue delay unless a legal exception applies.
10. Record all personal data breaches, including those that do not need to be reported, and document the decision and any lessons learned. <Cite refs=[['turn674984search9','turn674984search8']]>

14. Training, monitoring and accountability

All staff and volunteers will receive proportionate instruction on confidentiality, secure handling, child-specific privacy and reporting incidents. Additional guidance will be given to people who handle medical, safeguarding, recruitment or other sensitive records. Management will review access, supplier arrangements, privacy notices, retention practices and incident records periodically.

Where the nature, scope, context and purposes of processing require it, Activities 4 Kids will maintain records of processing activities, complete a DPIA and consult the ICO where required. Management will assess whether Activities 4 Kids meets the legal criteria for appointing a DPO; this policy does not assume that a DPO is mandatory.

15. Complaints and contact

Questions, concerns or rights requests should be directed to:

Designated data protection contact: Activities 4 Kids Management

Email: [insert monitored company privacy email]

Postal address: [insert company address]

ICO website: <https://ico.org.uk/>

Management must complete the contact fields above and ensure they are monitored before this policy is issued. Staff should report suspected breaches internally immediately and must not wait for a written complaint.

16. Related policies and legal framework

Read this policy alongside the Safeguarding and Child Protection Policy, Safe Recruitment Policy, Behaviour Management Policy, photo/video permissions, information-retention schedule, and any IT/security procedures.

- UK General Data Protection Regulation (UK GDPR), as amended.
- Data Protection Act 2018, as amended.



- Data (Use and Access) Act 2025 and relevant provisions in force.
- Privacy and Electronic Communications Regulations (PECR), where applicable.
- Current ICO guidance on children's information, individual rights, data security, data sharing, breaches and accountability.

Official ICO guidance on children's information was updated on 15 May 2026 to reflect the Data (Use and Access) Act 2025. Management should check current guidance before implementation, as regulatory guidance may continue to change. <Cite refs=[['turn674984search0','turn674984search5']]>/>

17. Approval and review

Policy approved by: Activities 4 Kids Management

Name / signature: _____

Date: 15 October 2026

Next review: 15 October 2027, or sooner following a legal change, significant incident, change to systems or data use, or Ofsted/ICO requirement.

Official guidance consulted

- ICO — Children and the UK GDPR — <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/>
- ICO — Personal data breaches: a guide — <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/>
- ICO — Data protection by design and by default — <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-by-default/>
- ICO — Data sharing and children — <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/data-sharing-and-children/>