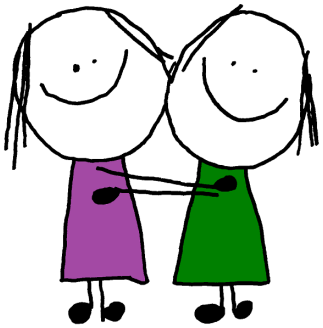
Friends – Play for Disabled Children



Friends – Play for Disabled Children
Email: info@friendsplay.org.uk
Website: www.friendsplay.org.uk
Registered Charity Number: 1167995

Data Protection Policy

Status: APPROVED by trustees (as confirmed 22 October 2026)
Version: 1.1
Approval date: 22 October 2026
Next review: October 2027 or sooner if required

Supersedes: Data Protection Policy version 1.0, approved 2 October 2026.

Earlier approved policies, including the June 2025 historical policy, should be retained in SharePoint version history or the charity archive.

1. Purpose

Friends – Play for Disabled Children ("Friends") is committed to protecting the personal information of the children, young people and families we support.

This policy explains how Friends collects, uses, stores, shares and deletes personal information and how trustees, volunteers and people acting on behalf of the charity are expected to handle it.

Friends processes information in accordance with the UK GDPR, the Data Protection Act 2018 and other relevant data-protection legislation.

A separate Family Privacy Notice explains our use of personal information to members and families in clear, accessible language.

2. Responsibility

Friends – Play for Disabled Children is the data controller for personal information collected for its charity activities.

The trustees are collectively responsible for ensuring that the charity complies with its data-protection responsibilities.

The charity's named Data Protection Lead is:

Paula Jones

Privacy and data-protection enquiries should be sent to:

info@friendsplay.org.uk

Day-to-day website and data administration may be carried out by authorised trustees and approved technical support providers.

3. Data we process

Depending on the activity, Friends may process:

- parent, carer and guardian names;
- email addresses, telephone numbers and postal addresses;
- Facebook/display names;
- emergency contact information;
- children's names and dates of birth;

- details of siblings and other relevant family members;
- membership and account information;
- transport requirements;
- bookings, orders, ticket quantities and attendance information;
- payment transaction information supplied through payment providers;
- photographs;
- email preferences;
- correspondence with families;
- funding and monitoring information;
- Nimbus/Access Card information, including cardholder name, card/reference number, expiry date and awarded access symbols;
- wheelchair, transfer and accessibility information;
- diagnoses and other health or disability information provided by families; and
- other information reasonably required to provide accessible activities safely and effectively.

Health and disability information is special-category personal data and is treated with additional care.

Friends does not routinely need or retain members' full bank or payment-card details. Online payments are processed through third-party payment providers.

4. Principles

Friends will:

- use personal information fairly, lawfully and transparently;
- collect information only for clear and legitimate purposes;
- collect only information reasonably necessary for those purposes;
- keep information accurate where reasonably possible;
- retain information only for as long as justified;
- keep personal information appropriately secure;
- restrict access to people who genuinely need it;
- give families clear information about how their data is used; and

- review the information we collect when processes change.

Particular care will be taken with children's information and health or disability information.

5. Purposes and lawful bases

Friends processes ordinary personal information for purposes including:

Membership administration

To assess and administer membership, maintain member accounts, communicate with families and provide charity services.

Friends will normally rely on its legitimate interests in administering the charity and providing services to its members, where those interests are not overridden by the rights and interests of the individuals concerned.

Orders and bookings

To take bookings, allocate tickets, arrange events and transport, issue information relating to bookings, administer refunds and maintain necessary transaction records.

Where a family purchases or books an activity, processing necessary to fulfil that booking may be carried out because it is necessary for the performance of the booking arrangement or contract.

Friends may also rely on legitimate interests where processing is necessary for associated charity administration.

Health, disability and accessibility information

Friends processes health and disability information where it is necessary to establish eligibility for the charity, understand access requirements, provide appropriate arrangements and support participation.

Routine health and disability information supplied as part of membership will normally be processed with the explicit consent of the relevant individual or, where appropriate, the person authorised to provide the information.

Where another special-category condition is required or more appropriate — for example in an exceptional safeguarding situation — Friends will identify and document the relevant condition before relying on it.

Friends will not rely simply on a person's agreement to a general privacy notice as explicit consent for special-category processing.

Event communications and marketing

Families may choose whether to receive emails notifying them about activities and events.

Where electronic marketing consent is required, Friends will use consent and members may withdraw that consent at any time.

Photographs

Photographs used for publicity will be managed in accordance with the information and permissions given to families.

Members of the Friends closed Facebook group are informed that photographs they post in the group may be reused by Friends for charity publicity, including on the Friends website, public Facebook page, newsletters and appropriate funding or promotional material.

Friends does not normally contact members again each time a photograph is selected for reuse where that reuse falls within the permission already given.

Families may contact Friends at info@friendsplay.org.uk if they want Friends to stop using a particular photograph on Friends-controlled channels. Friends will act on reasonable removal requests where practicable.

Funding, monitoring and statistics

Friends may analyse information about its membership and activities to demonstrate need, monitor reach and outcomes, and report to funders.

Where possible, information supplied externally for statistical or funding purposes will be aggregated or anonymised so that individual families cannot be identified.

Identifiable information will only be supplied where genuinely required and where Friends has a lawful basis to do so.

6. Special-category data

Health and disability information requires additional protection.

Friends will:

- collect only information reasonably necessary for the relevant purpose;
- avoid retaining full evidence where a verification record is sufficient;
- restrict access to authorised people;
- avoid unnecessary duplication;
- use secure systems for storage and transfer;
- document the applicable Article 9 condition;

- maintain any Appropriate Policy Document required by the Data Protection Act 2018; and
- keep special-category processing and retention under review.

Where explicit consent is relied upon, the consent must be specific, informed, clearly recorded and capable of being withdrawn.

Withdrawal of consent does not make earlier lawful processing unlawful.

7. Nimbus and eligibility information

Historically, families were able to upload disability/eligibility evidence through the website.

Friends has stopped routinely collecting and retaining full uploaded eligibility documents.

The registration form no longer requests the routine upload of full supporting evidence.

Where Friends needs ongoing Nimbus/Access Card information for accessible bookings, it will aim to retain only the information required operationally, such as:

- cardholder name;
- card/reference number;
- expiry date; and
- awarded access symbols.

Where a family emails evidence because it is required for verification, the evidence should be reviewed and the required verification details recorded. The original attachment and unnecessary duplicate copies should then be deleted as soon as they are no longer required.

Expired Nimbus details should be reviewed. Families may be contacted for an updated card and obsolete information should be removed when no longer needed.

8. Website and technical access

The Friends website is hosted by **34SP**.

The website uses WordPress and services/plugins required to administer membership, orders and bookings, including WooCommerce and membership/registration functionality.

Administrative access must be restricted according to need.

Routine administrative access is limited to authorised trustees and approved technical support.

Friends currently uses an independent technical developer for ongoing website support. That person has an individual account rather than sharing another administrator's credentials.

External plugin or software support providers may occasionally be given temporary access for troubleshooting or incident investigation. Such access must:

- be provided only where necessary;
- use an individual or controlled account where possible;
- be limited to the work being undertaken; and
- be removed when the work is complete.

Historic administrator access should be removed or reduced where it is no longer required.

9. Microsoft 365 and charity files

Friends uses Microsoft 365, including shared OneDrive/SharePoint storage.

Authorised users have their own logins. Shared charity information is stored within shared charity storage rather than through shared personal passwords.

Order exports, working spreadsheets, registers and other operational documents may be stored within the charity's Microsoft 365 environment.

Access will be limited according to operational need.

10. Orders and payments

Bookings and orders are administered through the Friends website, including WooCommerce.

Payments are processed through third-party payment providers such as PayPal and any other payment methods Friends may make available at checkout.

Friends does not need to receive members' complete bank-account or payment-card details.

Information retained by Friends may include order numbers, transaction references, payer/contact information, items purchased, quantities, refunds and other information required for booking and financial administration.

11. Email services

Friends uses its Microsoft 365 email accounts for ordinary charity correspondence.

Evidence or sensitive material received by email must not be retained indefinitely merely because it arrived by email.

Once information has been transferred to the appropriate charity record and the original attachment is no longer required, unnecessary duplicate copies should be deleted.

Friends also uses **EmailOctopus** for event/email communications. The mailing list is limited to the information required for that purpose, currently first name, surname and email address.

12. Microsoft Forms

Microsoft Forms may be used for surveys and feedback.

Feedback will normally be collected anonymously where identification is unnecessary.

Where respondents voluntarily provide details because they would like Friends to contact them, those details will be used for that purpose.

13. Sharing with venues and activity providers

Friends may need to provide limited information to venues, transport providers or activity providers in order to administer an event.

An ordinary attendance or admission register should contain only the information the provider genuinely requires, normally such as:

- lead-booker or family name;
- relevant ticket quantities; and
- any other booking information specifically required to deliver the activity.

Email addresses, telephone numbers, home addresses, diagnoses, Nimbus numbers or medical information must not be routinely included.

Additional accessibility information may be provided where it is genuinely necessary to arrange the member's access or participation.

14. AI and generative AI

Friends may use generative artificial-intelligence tools, including ChatGPT, to assist with appropriate charity administration.

Examples may include:

- drafting or improving communications;
- summarising non-sensitive information;
- organising administrative information;
- analysing booking data;
- identifying inconsistencies or anomalies;

- creating templates and planning documents; and
- supporting general charity administration.

The following rules apply.

Data minimisation

Personal information must be removed or reduced before being entered into an AI system wherever reasonably possible.

For example, order IDs or neutral family/reference codes should normally be used instead of names, email addresses, telephone numbers or postal addresses when analysing booking information.

Special-category information

Full Nimbus card images, DLA/PIP documentation, diagnostic reports, medical letters or similar evidence must not routinely be uploaded to an AI system.

Special-category or identifiable children's information should only be used where there is a specific, documented need, the information cannot reasonably be minimised further, and the proposed use is lawful and proportionate.

Files and exports

Before uploading spreadsheets or CSV files for analysis, unnecessary direct identifiers should be removed.

Free-text fields should be checked because they may contain names, contact information or health/disability information.

Human responsibility

AI outputs are advisory tools only. Decisions about members, eligibility, bookings, safeguarding or data-protection matters remain the responsibility of trustees or authorised people.

Sensitive decisions must not be made solely by an AI system.

Service settings and review

Friends should use appropriate privacy/data-control settings available within AI services and periodically review whether its use remains appropriate.

Turning off model-training settings is an additional safeguard but does not remove Friends' responsibilities under data-protection law.

15. Data processors and suppliers

Friends may use third-party suppliers that process personal information in providing services to the charity.

These may include:

- website hosting providers;
- website and technical support providers;
- WordPress/WooCommerce and related service providers;
- Microsoft 365;
- EmailOctopus;
- payment providers including PayPal;
- AI service providers where AI is used;
- venues, transport providers and event providers where necessary; and
- other professional or technical suppliers.

Friends will take reasonable steps to ensure that appropriate data-protection arrangements are in place with processors.

Implementation action — supplier assurances to verify: Maintain a supplier inventory recording each provider's actual role (processor, independent controller, or where supported joint controller), services and data categories, contract or data processing terms, subprocessors, security arrangements, location of processing and transfer safeguards, review date and outstanding evidence. Where Article 28 applies, verify documented instructions, confidentiality, security, subprocessors, assistance with rights/breaches, deletion or return, and audit information. Standard online agreements may suffice if their terms are appropriate. Do not represent supplier contracts or international safeguards as checked until evidence has been reviewed.

Where a provider processes data outside the UK, Friends will check that an appropriate lawful transfer mechanism or other permitted safeguard applies.

16. Retention

Friends will not retain personal information indefinitely merely because storage is available.

The following is the current retention approach:

Record	**Retention approach**
Active membership record	For the duration of membership

Inactive membership record	Delete after approximately 12 months of inactivity unless another lawful reason requires specific information to be retained
Full eligibility evidence	Delete after verification once no longer required; routine long-term storage is not intended
Nimbus/Access Card verification details	Retain while current and operationally required; review at expiry and remove obsolete details when no longer needed
Order/payment/accounting records	Retain for the period necessary for financial, accounting, audit, legal and funding requirements
Funded activity records	Retain for the period required by the relevant funding agreement/audit requirement, which may in some cases be up to seven years
Event registers	Retain only for as long as operationally, legally or contractually justified; where part of a funded/auditable activity, retain according to the relevant funding requirement
Routine correspondence	Delete when no longer required for the purpose for which it was received
Marketing list	Until the person unsubscribes, consent is withdrawn or the address is otherwise removed
Photographs/publicity	Review periodically and remove where no longer appropriate or following a reasonable withdrawal/removal request where Friends controls the publication

The trustees may document more specific periods as the charity's systems are further reviewed.

Paper records are subject to the same principles and must be stored securely.

Implementation action — retention controls to verify: Maintain a documented retention schedule with trigger, period, legal or funding exception, storage location, responsible reviewer and secure disposal method. Reconcile actual older membership, historical emails, HAF evidence, DBS material, funded registers and backups against the stated periods; no automatic bulk deletion of safeguarding, financial, incident, claims or in-

scope rights-request records. Establish a documented review and deletion process; log exceptions. Retention arrangements have not yet been fully verified as implemented.

17. Security

Friends will use proportionate organisational and technical measures to protect information.

These include, where appropriate:

- separate user accounts;
- strong passwords;
- restricted administrator access;
- secure cloud storage;
- limiting access according to role;
- keeping software reasonably up to date;
- removing obsolete accounts;
- secure transfer of sensitive information;
- avoiding unnecessary local copies;
- maintaining appropriate backups; and
- periodically reviewing access and security arrangements.

Sensitive documents should not be stored in insecure physical locations.

18. Personal data breaches

Any suspected loss, unauthorised disclosure, incorrect access, accidental publication or other personal-data security incident must be reported promptly to the trustees/Data Protection Lead.

Friends will:

1. contain the incident where possible;
2. preserve relevant evidence and logs;
3. establish what information and individuals may be affected;
4. assess the likely risk to individuals;
5. document the incident and decisions taken;
6. notify affected individuals where required; and

7. report the breach to the ICO within the applicable timeframe where the legal reporting threshold is met.

Incident documentation should be retained separately from ordinary membership information.

PROPOSED BREACH RESPONSE

All trustees, volunteers and authorised contractors should know to stop unsafe activity, protect affected people, report a suspected personal data breach immediately to Paula Jones (Data Protection Lead) using the charity contact route, and preserve relevant evidence. Paula and the trustees assess containment, nature/volume/sensitivity of information, likelihood and severity of harm, ICO reporting threshold and whether affected people must be notified. Where notifiable to the ICO, the normal statutory timeframe is without undue delay and where feasible within 72 hours of becoming aware. Document the incident, risk assessment, decisions, notifications, actions, owners, lessons and final verification in the restricted incident record. For technical incidents, supplier remediation and trustee sign-off must be independently confirmed; do not close them based only on a provider assurance.

19. Individual rights

Depending on the circumstances and lawful basis, individuals may have rights including:

- access to their personal information;
- correction of inaccurate information;
- erasure;
- restriction of processing;
- objection to processing;
- data portability;
- withdrawal of consent where processing relies on consent; and
- rights relating to automated decision-making.

Requests should be sent to:

info@friendsplay.org.uk

Friends will respond in accordance with the applicable legal requirements.

PROPOSED RIGHTS REQUEST PROCEDURE

Recognise requests received through any channel and refer promptly to Paula. Log request date, requester, category, identity/authority checks where genuinely needed, applicable deadline, searches, redactions/exemptions and response. Normally respond without undue delay and within one calendar month. Seek clarification promptly only where reasonably necessary, record any permitted pause; if complexity or numerous requests justify an extension, notify within the initial month and document why. Large volume alone is not sufficient. Search relevant charity systems, email including archives, SharePoint, paper records, relevant work devices and public/private messages where in scope. Preserve material once the request is received; never deliberately alter or delete it to avoid disclosure. Correct proven inaccuracies across affected systems and notify recipients when required; note disputed professional opinions appropriately. Assess erasure, objection, portability and restriction individually; safeguard children's interests, legal/financial obligations, third-party rights and backup arrangements. Provide accessible and secure replies; document valid grounds if refusing or charging a permitted fee and signpost ICO complaints.

20. Complaints

Anyone concerned about how Friends has handled their personal information should contact:

info@friendsplay.org.uk

They may also complain to the Information Commissioner's Office.

PROPOSED DATA PROTECTION COMPLAINTS PROCEDURE

Accept complaints by email, phone, in person or other reasonable channels. Anyone receiving one must promptly refer it to Paula as Data Protection Lead. Log date, issue, evidence, acknowledgement, investigation, decision, communication and remedial measures; provide a clear, accessible outcome and explain the right to contact the ICO. Preserve relevant incident and complaint records in appropriately restricted storage, and distinguish complaints about data use from ordinary event/customer feedback.

21. Review and approval

Implementation action — training and assurance: A named trustee should coordinate role-appropriate induction and refreshers for anyone handling Friends data. Cover privacy, minimisation, children's health/access information, sharing event lists, account/email security, retention, subject-access requests, complaints and urgent breach reporting; adapt for website administrators and event leads. Keep a restricted training record of participant, role, topics, date, evidence, results (if assessed), refresh date and follow-up. Recheck when technology, law or responsibilities change. Completion of one trustee's ICO course does not evidence organisation-wide training. Record approval and actual delivery separately.

This policy will be reviewed:

- at least annually;
- following a significant change to the charity's systems or data use;
- after a significant data-protection incident; or
- where relevant legislation or guidance changes.

Approved revised version: 1.1, 22 October 2026 (trustee approval confirmed by Emma). Next review: October 2027 or earlier following material change. Operational implementation and supplier evidence checks remain open and must not be treated as completed solely by this approval.