DATA PROTECTION & GDPR POLICY

Priority 1 Governance Document

Organisation	FND Connect
Status	Unincorporated Non-Profit Organisation
Address	133 Fable Lane, Kingswood, Hull, HU7 3PT
Document Code	FND-DATA-001
Version	1.0
Adopted	01/05/2026
Approved By	Matthew Gerdes-Hansen, Chair; Emma Wilder, Secretary
Review Cycle	As stated in this document

Controlled document. This policy should be read together with the FND Connect Constitution v1.0 and any supporting procedures adopted by the Management Committee.

Document Control

Owner	FND Connect Management Committee
Lead Responsible Person	As specified within this document
Adoption Date	01/05/2026
Review Cycle	Annual - next review 01/05/2027
Linked Constitution	FND Connect Constitution v1.0
Applies To	Committee Members, officers, volunteers, advisers, representatives and anyone acting

This document is drafted for FND Connect's current status as an unincorporated non-profit organisation and should be reviewed when FND Connect incorporates as a Community Interest Company, Charitable Incorporated Organisation or other legal entity.

1. Purpose

1.1 This Data Protection and GDPR Policy explains how FND Connect manages personal data and special category health information.

1.2 FND Connect recognises that people affected by FND may share sensitive information about diagnosis, seizures, mobility, symptoms, support needs, mental health, care arrangements and lived experience.

1.3 The purpose of this Policy is to ensure that personal data is handled lawfully, fairly, securely and transparently.

2. Scope

2.1 This Policy applies to Committee Members, officers, volunteers, moderators, advisers, contractors and anyone processing personal data for FND Connect.

2.2 It applies to information collected through website forms, email inboxes, Facebook groups and pages, online communities, Google Drive, iCloud, Dropbox or equivalent storage, spreadsheets, CRM systems, newsletter platforms, event forms, volunteer records and SeizeControl or future databases where applicable.

2.3 It applies to paper records and electronic records.

3. Data Protection Lead

3.1 The initial Data Protection Lead is Matthew Gerdes-Hansen.

3.2 The Data Protection Lead is responsible for coordinating data protection compliance, maintaining records, supporting data subject requests, managing incidents and advising the Committee.

3.3 FND Connect is not currently appointing a statutory Data Protection Officer unless legally required in future.

4. Types of Data Processed

4.1 FND Connect may process names, email addresses, telephone numbers, addresses, social media identifiers, website account details, enquiry information, volunteer applications, support group participation, newsletter preferences, event bookings, donation records and financial records.

4.2 FND Connect may process special category health information voluntarily provided by individuals, including FND diagnosis status, seizure information, symptoms, disability, mobility needs, support needs and related health information.

4.3 FND Connect shall collect only information reasonably necessary for its purposes.

5. Lawful Basis

5.1 FND Connect may rely on consent, legitimate interests, contract, legal obligation or vital interests depending on the activity.

5.2 For special category health information, FND Connect must identify an Article 9 condition under UK GDPR where required.

5.3 Potential Article 9 conditions may include explicit consent, provision of health or social care where applicable, not-for-profit body activities with appropriate safeguards, substantial public interest where applicable, or vital interests in emergency circumstances.

5.4 The appropriate lawful basis and condition shall be assessed according to the processing activity.

5.5 Consent must be freely given, specific, informed and capable of being withdrawn where relied upon.

6. Transparency and Privacy Notices

6.1 FND Connect shall provide appropriate privacy information to individuals.

6.2 A separate website Privacy Notice shall be produced and maintained.

6.3 Privacy information shall explain what data is collected, why it is used, legal basis, retention, sharing, rights and contact details.

6.4 Where data is collected through third-party platforms, the platform's own privacy terms may also apply.

7. Data Security

7.1 FND Connect shall use appropriate technical and organisational measures to protect personal data.

7.2 Measures may include strong passwords, multi-factor authentication, restricted access, secure storage, careful sharing, device security, access reviews and deletion of unnecessary data.

7.3 Health-related data shall be handled with heightened care.

7.4 Personal data shall not be stored on unsecured personal devices where avoidable.

7.5 Access shall be limited to those with a genuine need.

8. Data Sharing

8.1 FND Connect shall not sell personal data.

8.2 Personal data may be shared where necessary with service providers, email platforms, website hosts, cloud storage providers, payment providers, safeguarding agencies, emergency services, professional advisers, funders where anonymised or required, or regulators where legally required.

8.3 Safeguarding concerns may be shared without consent where necessary to protect a person from harm.

8.4 Data processing arrangements shall be reviewed where third-party providers are used.

9. Newsletter and Marketing

9.1 FND Connect plans to use Mailchimp or the cheapest compliant alternative for newsletters and communications.

9.2 Newsletter subscribers must be given clear information and an unsubscribe mechanism.

9.3 Marketing preferences shall be respected.

9.4 Suppression records may be retained to ensure unsubscribed individuals are not re-added.

10. Data Retention

10.1 FND Connect shall not retain personal data for longer than necessary.

10.2 Default retention periods are:

- General enquiries: 24 months.

- Volunteer records: 6 years after the role ends.

- Safeguarding records: 7 years, or longer if legally required.

- Financial records: 6 years.

- Newsletter records: until unsubscribe, plus suppression record.

- Health-related support information: no longer than necessary, default review after 24 months.

10.3 Retention periods may be extended where legal, safeguarding, insurance, funding or operational reasons justify this.

11. Individual Rights

11.1 Individuals may have rights to access, rectification, erasure, restriction, objection, portability and withdrawal of consent.

11.2 Requests should be directed to the Data Protection Lead.

11.3 FND Connect shall respond within legally required timescales unless an extension or exemption applies.

11.4 Identity may be verified before disclosure.

12. Data Breaches

12.1 A data breach may include loss, unauthorised disclosure, unauthorised access, accidental deletion, cyber compromise, misdirected email or improper sharing.

12.2 Suspected breaches must be reported promptly to the Data Protection Lead.

12.3 The Data Protection Lead shall assess risk and determine whether notification to the ICO or affected individuals is required.

12.4 Breach records shall be maintained.

13. Anonymised and Aggregated Data

13.1 FND Connect may use anonymised or aggregated data for research, service improvement, advocacy, impact reporting and education.

13.2 Data must be anonymised effectively before being treated as non-personal data.

13.3 Case studies and testimonials should not identify individuals unless clear consent has been obtained.

14. Review

14.1 This Policy shall be reviewed annually, or sooner following changes in law, systems, data use, service delivery or organisational structure.

14.2 The next scheduled review date is 01/05/2027.

Approval and Adoption

This Data Protection & GDPR Policy was approved and adopted by the Management Committee of FND Connect on 01/05/2026.

The document shall remain in force until amended, replaced or withdrawn by the Management Committee.

Signed by	Role	Signature	Date
Matthew Gerdes-Hansen	Chair		01/05/2026
Emma Wilder	Secretary		01/05/2026