DATA PROTECTION POLICY

Narthex Charity

Document Owner	Patricia Coleman-Taylor
Date Policy Implemented	June 2026
Owner Signature	Patricia Coleman-Taylor
Approved by	Narthex Trustees
Approval Date	June 2026
Review Date	12 months from Approval Date
Next Review Date	May 2027
What is this policy for?	This policy sets out how Narthex Charity complies with UK data protection law. It explains the principles we follow, the lawful basis on which we process personal data, the rights of the people whose information we hold, and the responsibilities of staff and volunteers who handle personal data in the course of their work.
Who is this policy for?	All employees, volunteers, trustees, and contractors of Narthex Charity. The policy also informs service users, donors, partners, and other individuals whose personal data Narthex processes.
Related documents	Service User Rights and Responsibilities Policy; Referral and Signposting Policy; Safeguarding Policy and Procedures; Satellite Partnership Policy; Complaints Policy and Procedure; Disciplinary Policy; Grievance Policy; Whistleblowing Policy; Equality, Diversity and Inclusion Policy.

1. Policy Statement

Narthex Charity processes personal data about service users, employees, volunteers, donors, partners, and members of the public as part of its charitable work. We are committed to handling that data responsibly, in accordance with UK data protection law and with respect for the rights of the people whose information we hold.

Narthex Sparkhill is registered with the Information Commissioner's Office (ICO) as a data controller. The charity takes data protection seriously because the information we hold about people is often sensitive, and because mishandling it could cause real harm, particularly to service users who are already in crisis.

This policy sets out how we meet our obligations and how staff and volunteers should handle personal data in practice.

2. Scope

This policy applies to:

- All personal data processed by Narthex, in any format - electronic, paper, voice recording, photographic or video image, or any other form.
- All activity where Narthex is the data controller, including services delivered at the main site, at satellites, by telephone, or online.
- All employees, volunteers, trustees, and contractors of Narthex who handle personal data in the course of their role.

'Personal data' means any information relating to an identified or identifiable individual. 'Processing' includes any operation on personal data, including collection, storage, use, disclosure, and disposal.

3. Legal Framework

This policy reflects Narthex's obligations under:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018 (DPA 2018), which supplements UK GDPR for UK-specific provisions and derogations.
- The Data (Use and Access) Act 2025 (DUAA), which amends the UK GDPR, the Data Protection Act 2018, and PECR, with provisions commencing in stages during 2026.
- The Privacy and Electronic Communications Regulations 2003 (PECR), which govern marketing communications by electronic means.
- The Human Rights Act 1998, particularly Article 8 (right to private and family life).
- Sector-specific guidance from the ICO for charities and small organisations.

4. Key Concepts and Definitions

4.1 Data Controller

A data controller is the organisation that determines the purposes and means of processing personal data. Narthex is the data controller for personal data it processes for its own charitable purposes, including data about service users, employees, volunteers, donors, and supporters.

4.2 Data Processor

A data processor is an organisation that processes personal data on behalf of a controller. Narthex acts as a processor in limited circumstances. Satellite food bank partners act as processors on behalf of Narthex in relation to food bank data, as set out in the Satellite Partnership Policy.

4.3 Personal Data

Any information relating to an identified or identifiable individual. This includes names, addresses, contact details, identification numbers, photographs, voice recordings, IP addresses, and any information that, combined with other data, could identify a person.

4.4 Special Category Data

Certain categories of data receive additional protection under Article 9 UK GDPR. These are: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data where used for identification; data concerning health; data concerning sex life or sexual orientation. Criminal offence data is also specially protected under Article 10.

Narthex processes special category data where necessary for its charitable work - for example, health information shared by service users for dietary or support purposes; religious information relevant to cultural or dietary requirements; or safeguarding information relating to the wellbeing of service users, staff, or volunteers. This processing is subject to additional legal conditions as set out in Section 6.

4.5 Data Subject

The identified or identifiable individual to whom the data relates - for Narthex, typically a service user, employee, volunteer, or member of the public.

4.6 Processing

Any operation performed on personal data, including: collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, restriction, erasure, or destruction.

5. Data Protection Principles

Narthex processes personal data in accordance with the seven principles set out in Article 5 UK GDPR:

5.1 Lawfulness, Fairness, and Transparency

Personal data is processed lawfully, fairly, and in a way that is transparent to the individual. Narthex identifies a lawful basis (see Section 6) for every processing activity and provides privacy information so people understand how their data is used.

5.2 Purpose Limitation

Personal data is collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes. Where Narthex wishes to use data for a new purpose, it considers whether the new purpose is compatible with the original, and seeks fresh consent where it is not.

5.3 Data Minimisation

Personal data collected is adequate, relevant, and limited to what is necessary for the purpose. Narthex does not collect data 'just in case'.

5.4 Accuracy

Personal data is accurate and, where necessary, kept up to date. Inaccurate data is corrected or erased without delay. Service users and employees are asked to let Narthex know when their details change.

5.5 Storage Limitation

Personal data is kept in a form that permits identification of individuals for no longer than is necessary. Narthex's retention schedule is at Appendix A.

5.6 Integrity and Confidentiality (Security)

Personal data is processed securely, protecting against unauthorised or unlawful processing, accidental loss, destruction, or damage, through appropriate technical and organisational measures. See Section 13.

5.7 Accountability

Narthex is responsible for complying with UK GDPR and can demonstrate that compliance. This is achieved through this policy, records of processing activities, data protection impact assessments where appropriate, training, and governance arrangements set out in Section 7.

6. Lawful Basis for Processing

Narthex identifies a lawful basis under Article 6 UK GDPR for every processing activity. The six bases are:

6.1 Consent

The individual has given clear, informed, specific consent to the processing for a specific purpose. Consent is freely given, unambiguous, and recorded. It can be withdrawn at any time. Narthex uses consent for processing such as marketing communications, photography for publicity, and certain referrals.

6.2 Contract

Processing is necessary for a contract with the individual, or to take steps at their request before entering a contract. Narthex uses this basis for processing relating to employment contracts and certain supplier arrangements.

6.3 Legal Obligation

Processing is necessary to comply with a legal obligation. Narthex uses this basis for HMRC reporting, employment law compliance, and certain statutory reporting obligations (for example, safeguarding duties and Charity Commission reporting).

6.4 Vital Interests

Processing is necessary to protect someone's life. Narthex may use this basis in medical emergencies or other situations where failing to process data would risk a person's life.

6.5 Public Task

Processing is necessary to perform a task in the public interest or in the exercise of official authority. Narthex uses this basis in limited circumstances where it is acting under specific legal authority.

6.6 Legitimate Interests

Processing is necessary for a legitimate interest of Narthex or a third party, which is not overridden by the individual's rights and freedoms. Narthex uses this basis for much of its routine operation of charitable activity, after carrying out a legitimate interests assessment to ensure the balance falls in favour of processing.

6.7 Special Category Data Conditions

Where Narthex processes special category data, an additional Article 9 UK GDPR condition applies. Common conditions relied on by Narthex are:

- Explicit consent from the individual.
- Vital interests, where consent cannot be given.
- Not-for-profit bodies processing data of members or regular contacts.
- Processing necessary for reasons of substantial public interest under specific safeguards (for example, safeguarding of children and individuals at risk).
- Processing for the establishment, exercise, or defence of legal claims.

Where a substantial public interest condition under Schedule 1 of the DPA 2018 is relied on (for example, the safeguarding condition), Narthex has an Appropriate Policy Document that sets out how the processing complies with principles and how retention is managed. This Data Protection Policy, together with the Safeguarding Policy, forms the Appropriate Policy Document for Narthex's safeguarding processing.

7. Roles and Responsibilities

7.1 Data Protection Lead

Narthex has appointed a Data Protection Lead to serve as the internal point of contact for data protection matters. The Data Protection Lead is Geoff Holt, Trustee.

Narthex has considered whether it is required to appoint a statutory Data Protection Officer under Article 37 UK GDPR. Narthex's core activities do not involve large-scale regular and systematic monitoring, and while special category data is processed, the scale is not such that a statutory DPO is required. The Data Protection Lead is therefore a non-statutory internal role, not a statutory DPO. This position is reviewed annually as part of the policy review.

The Data Protection Lead is responsible for:

- Serving as the internal point of contact for data protection queries from staff, volunteers, and data subjects.
- Maintaining oversight of Narthex's records of processing activities.
- Handling data subject rights requests, including subject access requests.
- Coordinating responses to personal data breaches and ICO notifications where required.
- Operating the data protection complaints process, including acknowledging, investigating, and responding to complaints within the required timescales.
- Approving processing of personal data for purposes outside routine operation.
- Reviewing data sharing arrangements with partners and processors.
- Ensuring data protection training is provided and recorded.
- Reporting to Trustees on data protection matters, including breaches, subject access requests, and any systemic issues.
- Where complex matters arise, seeking advice through Avensure or other appropriate external specialist support.

7.2 Trustees

The Board of Trustees holds overall accountability for data protection at Narthex. Trustees approve this policy, receive regular reports from the Data Protection Lead, and consider data protection as part of risk management oversight.

7.3 Line Managers

Line managers ensure that the employees and volunteers they manage understand and apply this policy. They escalate queries and concerns to the Data Protection Lead where appropriate, and ensure their teams complete required training.

7.4 All Employees, Volunteers, Trustees, and Contractors

Everyone who handles personal data on behalf of Narthex is responsible for:

- Following this policy and any associated procedures.
- Completing data protection training and refresher training.
- Reporting personal data breaches, near misses, or concerns without delay.
- Only accessing personal data where there is a legitimate business reason to do so.
- Keeping passwords confidential, following secure working practices, and protecting data both at the main site and at any remote or satellite location.

8. Transparency and Privacy Information

Narthex tells people what we do with their data. Privacy information includes who we are, what data we collect, why, how long we keep it, who we share it with, what rights the individual has, and how to contact us or the ICO.

8.1 Service Users

Service users are given privacy information on registration for a Narthex service. Where the interaction is in person, a signature is obtained to confirm understanding. For telephone registration, the information is given verbally and a note is recorded that this has happened. Privacy notices are also displayed at each Narthex site and available on request.

8.2 Employees and Volunteers

Employees receive privacy information as part of their contract of employment and induction. Volunteers receive equivalent information at the start of their volunteering. Updates are communicated in writing.

8.3 Donors, Supporters, and Others

Privacy information for donors and supporters is provided at the point of contact (donation form, sign-up form, website). The Narthex website includes a privacy notice covering all routine interactions with the public.

9. Data Subject Rights

Under UK GDPR, individuals have eight rights in relation to their personal data. Narthex respects and enables these rights.

9.1 Right to Be Informed

Individuals have the right to be told how their data is processed, through the privacy information in Section 8.

9.2 Right of Access (Subject Access)

Individuals have the right to know what personal data Narthex holds about them, to see that data, and to receive a copy. Requests are handled within one month of receipt, extendable by a further two months for complex requests. There is normally no fee. The Data Protection Lead handles subject access requests.

9.3 Right to Rectification

Individuals can ask for inaccurate or incomplete data about them to be corrected.

9.4 Right to Erasure

Individuals can ask for their data to be erased in certain circumstances - for example, where it is no longer needed, where consent is withdrawn, or where it was processed unlawfully. The right is not absolute; Narthex may retain data where there is a legal obligation or other lawful basis.

9.5 Right to Restrict Processing

Individuals can ask Narthex to restrict how their data is used in certain circumstances - for example, while the accuracy of data is being verified.

9.6 Right to Data Portability

Where data is processed on the basis of consent or contract and by automated means, individuals can ask for it to be provided in a structured, commonly used, machine-readable format, or transferred to another controller where technically feasible.

9.7 Right to Object

Individuals can object to processing based on legitimate interests, public task, or direct marketing. Objections to direct marketing are absolute. Objections on other grounds are considered against Narthex's legitimate grounds to continue processing.

9.8 Rights Relating to Automated Decision-Making

Individuals have rights where decisions affecting them are made by automated means including profiling. Narthex does not currently use automated decision-making of this kind.

9.9 How to Exercise Rights

Requests under any of the above rights are made to the Data Protection Lead, by email, letter, or in person. Narthex responds to all rights requests within the statutory timescales. No charge is made for routine requests. Requests are logged in the Data Protection Lead's record of subject access and rights activity.

9.10 Right to Complain

Individuals have the right to complain directly to Narthex if they believe we have handled their personal data in a way that breaches data protection law. A data protection complaint is any expression of dissatisfaction about how we have handled a person's own personal data. We accept complaints however they reach us, including by email, letter, telephone, or in person, and they do not have to be made on a particular form. Complaints are directed to the Data Protection Lead.

On receiving a data protection complaint, Narthex:

- acknowledges receipt within 30 days;
- makes appropriate enquiries into the complaint and keeps the complainant informed of progress;
- provides the outcome without undue delay, in plain language; and
- records the complaint, the steps taken, and the outcome.

Narthex aims to provide the outcome of a complaint within one month, in line with how it handles subject access requests, and will explain if a complaint is complex and needs

longer. If the complainant remains dissatisfied, they may complain to the ICO, who will normally expect the complaint to have been raised with Narthex first. This duty is set out in section 164A of the Data Protection Act 2018, inserted by the Data (Use and Access) Act 2025, and applies from 19 June 2026.

10. Records of Processing Activities

Under Article 30 UK GDPR, Narthex maintains a record of its processing activities (ROPA). The ROPA is held by the Data Protection Lead and includes, for each category of processing:

- The purpose of the processing.
- Categories of data subjects and personal data.
- Categories of recipients to whom data is or will be disclosed.
- Any international transfers and associated safeguards.
- Retention periods.
- A general description of technical and organisational security measures.

The ROPA is reviewed at least annually by the Data Protection Lead.

11. Data Protection Impact Assessments (DPIAs)

A DPIA is carried out before Narthex begins any new processing activity that is likely to result in a high risk to individuals' rights and freedoms. This includes:

- New systems that involve large-scale processing of special category data.
- Systematic monitoring of individuals.
- Processing that may result in denial of service or significant effect on individuals.
- Changes to existing processing that significantly alter the scale, nature, or purpose of processing.

The DPIA process is led by the Data Protection Lead with input from relevant staff. Where a DPIA identifies residual high risk that cannot be mitigated, Narthex consults the ICO before starting the processing.

12. Access to Personal Data Within Narthex

Personal data is accessed on a 'need to know' basis. Ability to access does not imply a right to use. Roles that access personal data do so only for the purpose of their role. Examples:

- Staff and volunteers delivering services access service user data only as needed for that service.
- The Chief Executive and line managers access employee and volunteer data as needed for management and safe delivery.
- The Accounts Assistant and Finance Manager access data needed for finance and payroll.
- The Designated Safeguarding Lead accesses safeguarding records.
- The Data Protection Lead accesses data to respond to rights requests and investigate breaches.

Different Microsoft 365 permission levels apply to different role types. Changes to access are requested by the relevant line manager and approved by the Chief Executive.

Narthex will share personal information with the relevant authorities where this is in the public interest, regardless of consent, where there are actual or potential concerns about the

safety of any individual or group - for example, under safeguarding duties, adult support and protection, mental welfare, modern slavery, or in connection with illegal activity. In such cases, the Manager refers first to the relevant policy (Safeguarding, Whistleblowing, or similar). Where the situation is not explicitly covered by another policy, the Manager consults the Data Protection Lead.

In an emergency where a person has been harmed or is at risk of harm, Narthex gives authorities the information they need to respond. Consultation with the Data Protection Lead is done at the earliest opportunity after the emergency.

13. Security

Narthex protects personal data through technical and organisational measures appropriate to the risk.

13.1 Paper Records

- Stored in lockable cabinets when not in use, with keys held securely.
- Not left on desks or screens when the workspace is unattended.
- Returned to secure storage after use.
- Archived according to the retention schedule in Appendix A.
- Disposed of securely at the end of the retention period, by shredding or through a secure waste disposal contract.

13.2 Electronic Records

- Stored within the Microsoft 365 environment (see Section 14 on international transfers).
- Protected by individual user passwords that are unique, regularly updated, and not shared.
- Access levels aligned with role, controlled by the Chief Executive.
- Multi-factor authentication applied where available, particularly for accounts with elevated access.
- Sensitive data shared externally only with encryption or password protection.
- Devices (laptops, phones) protected by password and, where available, encryption.

13.3 Incoming and Outgoing Post and Print

- Incoming post marked personal is opened only by the addressee.
- Outgoing post is checked before sending to ensure correct recipient and enclosures.
- Confidential documentation is placed in a separate inner envelope before the main envelope.
- Printed documents are collected promptly and disposed of securely if not collected within five minutes.

13.4 Remote and Flexible Working

Staff and volunteers working remotely (from home, at a satellite, or at a partner location) protect personal data to the same standard as at the main site. This includes using only Narthex-approved devices and accounts, not saving personal data on personal devices or personal cloud storage, and ensuring that printed material is kept secure and disposed of properly.

13.5 Satellites

At satellite food bank sites, the Satellite Partnership Policy and the data processing addendum in the Partnership Agreement set out the security requirements. Personal data at satellites is processed through Narthex systems (primarily the Trussell Data Collection System and secure email) rather than satellite-owned systems.

14. International Transfers of Personal Data

Narthex does not routinely transfer personal data outside the United Kingdom for its own charitable purposes. However, Narthex uses Microsoft 365 for email, document storage, and collaboration. Microsoft's services involve processing of data across Microsoft's global infrastructure, which may include locations outside the UK.

This international transfer is lawful under UK GDPR on the following basis:

- Microsoft operates data centres in the UK and EU, and Narthex's tenant configuration uses UK and EU data residency for stored content where available.
- The European Union has been granted adequacy status by the UK under the UK GDPR, meaning transfers to EU locations do not require additional safeguards.
- For transfers to locations outside the UK and EU, Microsoft provides standard contractual clauses and the UK International Data Transfer Addendum as part of its Online Services Terms, which Narthex has accepted as part of its Microsoft subscription.
- Microsoft's Data Protection Addendum and Online Services Terms form the basis of the contractual relationship and include commitments that apply to personal data processed by Microsoft on Narthex's behalf.

Where Narthex adopts any other cloud service or third-party processor in future, the Data Protection Lead reviews the provider's data handling arrangements before adoption, including any international transfer implications.

Where Narthex transfers personal data to another organisation for its own charitable purposes (for example, a referral to a partner organisation), this is handled under the Referral and Signposting Policy. Such transfers are almost always within the UK.

15. Personal Data Breaches

15.1 What Is a Personal Data Breach

A personal data breach is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- A lost or stolen laptop, phone, or paper file containing personal data.
- An email sent to the wrong recipient that contains personal data.
- Unauthorised access to Narthex systems or files.
- A Narthex account compromised by phishing or credential theft.
- Accidental disclosure of personal data in a group email or publication.

15.2 Reporting Breaches Internally

Anyone who discovers or suspects a personal data breach must report it to the Data Protection Lead immediately, and in any event within 24 hours. Reports are made in writing (by email is acceptable) and include:

- What happened.

- When it happened, and when it was discovered.
- What data is affected, and how many individuals may be affected.
- Any immediate action already taken.

Reporting a breach is not itself a disciplinary matter. Narthex wants people to report breaches early so they can be contained. Concealing a breach is a serious matter and may be a disciplinary issue.

15.3 Breach Response

On receipt of a breach report, the Data Protection Lead:

- Takes immediate action to contain the breach and limit harm.
- Assesses the risk to affected individuals.
- Decides whether to notify the ICO and whether to notify affected individuals.
- Records the breach in the breach register.
- Identifies lessons learned and any policy or practice changes needed.

15.4 ICO Notification

A personal data breach that is likely to result in a risk to the rights and freedoms of individuals is notified to the ICO without undue delay and, where feasible, within 72 hours of Narthex becoming aware of it. Narthex reports via www.ico.org.uk. The notification includes:

- The nature of the breach and the categories and approximate number of individuals and records affected.
- The name and contact details of the Data Protection Lead.
- The likely consequences of the breach.
- Measures taken or proposed to address the breach.

Where Narthex does not notify within 72 hours, the reasons for the delay are documented. Not every breach needs to be reported - the test is risk to rights and freedoms.

15.5 Notification to Affected Individuals

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those individuals are notified directly without undue delay. The notification explains:

- The circumstances of the breach.
- The details of the Data Protection Lead managing the breach.
- Actions Narthex has taken and proposes to take.
- Any steps the individual can take to protect themselves.

15.6 Breach Register

The Data Protection Lead maintains a central register of all personal data breaches, whether or not notified to the ICO. The register records the breach, the response, and any lessons learned. The register is reviewed periodically for patterns and reported to Trustees.

16. Direct Marketing and Fundraising

Where Narthex communicates with individuals for fundraising, supporter engagement, or similar marketing purposes, it complies with both UK GDPR and the Privacy and Electronic Communications Regulations (PECR).

Marketing communications by email, text message, or automated call require the individual's prior consent, obtained on an opt-in basis, unless an exemption applies. As a charity, Narthex may rely on the charitable purpose soft opt-in introduced by the Data (Use and Access) Act 2025. This allows Narthex to send marketing emails and texts to further its charitable purposes where it obtained the person's contact details when they expressed an interest in, or offered support to, those purposes, and where the person was given a simple way to opt out at that point and in every message since. Narthex applies the soft opt-in only where all conditions are met, and continues to follow the Code of Fundraising Practice. Marketing by post and live phone call operates on an opt-out basis, and Narthex respects any individual who opts out.

Individuals can withdraw consent at any time and Narthex acts on withdrawal without delay. Every marketing communication includes a clear opt-out route. Narthex maintains suppression lists to ensure that people who have opted out do not receive further marketing.

17. Consent

Where Narthex relies on consent as the lawful basis for processing (rather than another Article 6 basis), the consent is:

- Freely given - not required as a condition of receiving a service, where the service can be delivered without the processing.
- Specific - to a particular processing purpose, not bundled.
- Informed - the person is told what they are consenting to.
- Unambiguous - expressed by a clear affirmative act (not silence, pre-ticked boxes, or inactivity).
- Documented - a record of the consent is kept.
- Withdrawable - the person can withdraw consent as easily as they gave it.

Where consent is for special category data, it must additionally be explicit - a clear statement of consent, not inferred from context.

18. Disclosure of Personal Data Outside Normal Purpose

Narthex may be asked to disclose personal data for purposes other than those for which it was originally collected. Common scenarios include:

18.1 Information Requests in Support of Individuals

For example, a request to provide a reference for a service user applying for housing, employment, or a financial product. Narthex will only provide such information with the written consent of the person to whom the data relates. A copy of the consent is retained with the request.

18.2 Information Requests for Official Investigation

For example, a police inquiry or request from a statutory body under specific legal authority. The Data Protection Lead assesses the request and confirms the legal basis before any disclosure. Where a request is for data in connection with a criminal investigation, Narthex may disclose without informing the individual where doing so would prejudice the investigation. A written rationale for any disclosure without consent is retained on file.

18.3 Safeguarding

Disclosure of data in connection with a safeguarding concern is handled under the Safeguarding Policy, with appropriate legal basis as set out in Section 6.

18.4 Staff Who Receive Unusual Requests

A staff member or volunteer who receives a request for personal data that exceeds what their role usually handles (for example, a subject access request, a request from a lawyer, or a request from a regulator) escalates the request to their line manager, who routes it to the Data Protection Lead.

19. Training and Awareness

All new employees and volunteers receive data protection awareness as part of their induction, covering the principles, their individual responsibilities, how to recognise and report a breach, and how to handle subject access requests.

Refresher training is provided periodically and after any significant change to this policy or to data protection law. The Data Protection Lead maintains a training register recording who has received training and when.

Line managers are additionally briefed on their responsibilities, including data access requests, breach response, and routine decisions on sharing information.

20. Interfaces with Other Policies

This policy sits alongside and supports several other policies in the Narthex suite:

Service User Rights and Responsibilities Policy: sets out service users' rights in relation to their personal data.

Referral and Signposting Policy: provides detailed UK GDPR provisions for data sharing with referral partners.

Safeguarding Policy and Procedures: sets out information sharing provisions for safeguarding, including the lawful basis and conditions.

Satellite Partnership Policy: sets out the controller-processor relationship with satellite partners, with the data processing addendum in the Partnership Agreement.

Complaints, Disciplinary, Grievance, Whistleblowing Policies: each contain provisions on record keeping and retention consistent with this policy.

Communications and Social Media Policy: sets out handling of photographs, images, and communications, which is informed by this policy.

21. Review

This policy is reviewed annually by the Document Owner, and earlier where there are significant changes in law, regulator guidance, Narthex's processing activities, or the information systems Narthex uses. Review considers:

- Changes in UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, PECR, or ICO guidance.
- Any breaches during the year and lessons learned.
- Any subject access or rights requests and the handling of them.
- Changes to Narthex's systems, services, or partnerships that affect data processing.
- Whether the decision not to appoint a statutory DPO remains appropriate.

Appendix A: Retention Schedule

This appendix sets out retention periods for the main categories of personal data Narthex processes. Retention is based on legal and regulatory requirements, operational need, and the data minimisation principle. Periods are measured from the trigger event identified in the table.

Where a retention period below differs from a provision in another policy, this schedule takes precedence unless the other provision is supported by a specific legal obligation. Retention periods are reviewed as part of the annual policy review.

Data category	Retention period	Legal or operational basis
Service user records (food bank, advice, community activities)	6 years after last contact	Operational basis; aligned with broader contract-type limitation periods; supports continuity where a service user returns
Food bank voucher records (DCS)	Per Trussell DCS retention policy (typically 3 years)	Trussell Trust member requirements and DCS data handling
Advice service case files	6 years after case closure	Standard advice sector practice; supports follow-up complaints and audit
Safeguarding records	Indefinitely, subject to periodic review	Legal and regulatory expectation; supports response to historical safeguarding inquiries
Safeguarding Incident Register (summary)	Indefinitely	Governance record
Complaints records	6 years after conclusion	Complaints Policy
Complaint records (safeguarding-related)	Indefinitely, subject to periodic review	Aligned with safeguarding
Employee records (HR file)	6 years after end of employment	Employment law limitation periods; HMRC requirements
Payroll and tax records	6 years after end of tax year	HMRC requirement
Pension records (where applicable)	Indefinitely, subject to pension trustee requirements	Statutory requirement
Volunteer records	2 years after end of volunteering	Operational basis; ability to provide references
Disciplinary records	2 years after end of employment or volunteering	Disciplinary Policy

Grievance records	2 years after conclusion	Grievance Policy
Whistleblowing records	6 years after conclusion	Whistleblowing Policy; public interest retention
Recruitment records - unsuccessful candidates	6 months after decision	Default period for potential discrimination claims; ICO guidance
Recruitment records - successful candidate	Folded into employee record at appointment	Becomes part of the HR file
DBS check information	6 months after DBS decision	DBS Code of Practice
Donor records	6 years after last donation or contact	Gift Aid and tax compliance; relationship continuity
Marketing consent records	Until consent withdrawn plus 2 years	Evidence of consent in the event of a challenge
Supplier and contractor records	6 years after end of contract	Contract law limitation periods
Financial and accounting records (non-personal)	6 years after end of financial year	Companies Act and HMRC requirements
CCTV footage (where in use)	30 days, unless needed for investigation	ICO guidance for CCTV in small organisations
Minutes of Trustee meetings	Indefinitely	Charity governance record
Policies and policy review records	Indefinitely	Governance
Personal data breach register	6 years after breach closure	Accountability principle; ICO expectation

Notes:

- 'Last contact' for service users means the most recent interaction of any kind (appointment, voucher fulfilment, correspondence).
- Special category data (health, religious belief, ethnicity, safeguarding status) receives the same retention as the surrounding record but is reviewed with particular care at the end of the period.
- Where a legal proceeding, regulatory inquiry, or complaint is live, relevant records are preserved until the matter concludes, regardless of the routine retention period.
- Retention periods are minimum periods where driven by legal obligation, and maximum periods where driven by data minimisation. Narthex reviews active case files periodically and deletes data that is no longer needed, without waiting for the maximum period.
- Secure destruction at end of retention: paper records are shredded in-house or via secure waste contract; electronic records are deleted from live and backup systems.