Focusing on Ability

DEMENTIA ACTIVE

Confidentiality, Privacy, Data Protection and Cyber Security Policy

Policy owner	Andrew Gill, Chief Executive Officer
Applies to	Dementia Active Community Interest Company and Dementia Active CIO (the charity)
Original policy record	Andrew Gill, 8 June 2026; approved by the Trustees, as recorded in the existing policy
Existing scheduled review date	7 June 2027
Previous website wording updates	12 October 2026
Consolidated website draft prepared	25 October 2026

The 12 October 2026 updates clarified complaints, controller responsibilities and information sharing. This consolidated rewrite retains those updates and incorporates cyber security requirements. It does not itself record fresh trustee or director approval. Approval of this consolidated version must be recorded separately by the relevant governing bodies.

Contents

1. Our commitment . . . 3
2. Who this policy covers . . . 3
3. The organisations responsible for information . . . 3
4. Contact details . . . 4
5. Personal information we collect . . . 4
6. Where information comes from . . . 4
7. Why we use personal information . . . 5
8. Our lawful bases for using information . . . 5
9. Health and other sensitive information . . . 6
10. Consent, capacity and representatives . . . 6
11. Photographs, videos and publicity . . . 6
12. Sharing personal information . . . 7
13. Sharing between the CIC, CIO and volunteers . . . 7
14. Jotform and online forms . . . 8
15. Service providers and overseas processing . . . 8
16. Staff, volunteer and applicant information . . . 9
17. Retention and secure disposal . . . 10
18. Your data protection rights . . . 10
19. Handling rights requests . . . 11
20. Marketing, website information and cookies . . . 11
21. Confidentiality and secure handling . . . 11
22. Cyber security safeguards . . . 12
23. Working away from premises . . . 12
24. Safeguarding and information sharing . . . 13
25. Recognising and reporting security incidents . . . 13
26. Cyber attack and breach response . . . 13
27. Breach assessment and notifications . . . 14
28. Member safety, transport and business continuity . . . 14
29. Recovery, incident records and communications . . . 15
30. Responsibilities, training and oversight . . . 15
31. Privacy complaints and the ICO . . . 16
32. Policy review, document control and approval . . . 17

1. Our commitment

Dementia Active respects the privacy, dignity and confidentiality of everyone who uses, works with or supports our services.

This policy explains how we collect, use, share, store and protect personal information. It explains people's rights and the responsibilities of staff, volunteers, trustees, directors and contractors.

We handle information in accordance with applicable UK data protection law, including the UK General Data Protection Regulation, the Data Protection Act 2018 and subsequent amendments.

We recognise that information about dementia, health, care needs, safeguarding, home addresses and transport arrangements requires particular protection. Its loss, misuse or disclosure could affect an individual's safety and wellbeing.

2. Who this policy covers

This policy covers information about:

- People attending our groups, sessions and activities.
- Relatives, friends, carers, representatives and emergency contacts.
- Staff, volunteers, trustees, directors, contractors and applicants.
- Donors, supporters, referrers and professional partners.
- Website visitors and people contacting us.
- Organisations arranging Dementia Active sessions or services.

It applies to electronic records, paper documents, photographs, videos, online forms, email, messaging, telephone calls and verbal conversations.

It applies at our premises, community venues, in vehicles, at home and wherever organisational information is accessed.

3. The organisations responsible for information

Dementia Active Community Interest Company, registration number 11973554, is the data controller for the registration, participant and member information it collects and uses, including enquiries submitted through the Didcot interest form.

A data controller decides why personal information is needed and how it is used.

All donations go to Dementia Active CIO, charity number 1195246. The CIO handles information needed for its charitable activities, donation administration and Gift Aid.

Each organisation is responsible for the information it controls. The organisation employing a staff member or engaging a volunteer is responsible for its employment or volunteering records.

The CIC and CIO must not assume that sharing a name, personnel or systems permits unrestricted sharing of information. Where responsibilities overlap, the organisations must document their respective roles and any necessary sharing arrangements.

4. Contact details

For privacy questions, rights requests, complaints or security concerns, contact:

Dementia Active

7 Manor Park

Jugglers Close

Banbury

Oxfordshire

OX16 3TB

Telephone: 01295 408441

Email: info@dementiactive.co.uk

Alternative email: dementiactive@gmail.com

Please ask for Andrew Gill or the person responsible for data protection. Where possible, tell us whether your enquiry concerns the CIC, the CIO or both.

If you suspect an email account has been compromised, telephone us using a number you already know to be correct.

5. Personal information we collect

We collect information relevant to our relationship with an individual and the services we provide. This may include:

- Names, addresses, telephone numbers and email addresses.
- Dates of birth and communication preferences.
- Details of relatives, carers, representatives and emergency contacts.
- Information about health, dementia, mobility, allergies, medication and support needs.
- Attendance, activities, transport and collection arrangements.
- Risk assessments, accidents, incidents, safeguarding concerns and complaints.
- Payment, donation and Gift Aid information.
- Photographs, videos and personal stories where appropriate permission has been obtained.
- Recruitment, employment, volunteering, payroll, pension, training, expenses and wellbeing records.
- Information submitted through our website or online forms.
- Technical website information where collected by our hosting or other approved providers.

We must collect only information necessary for a defined purpose. Staff must avoid recording unnecessary personal opinions or unrelated details.

6. Where information comes from

Information may come directly from the individual or from a relative, friend, carer, authorised representative, referrer, employer, professional partner or public authority.

It may be collected through conversations, registration forms, Jotform, correspondence, service records, payment arrangements or recruitment processes.

Where someone gives us information about another person, we must consider their authority to do so and provide appropriate privacy information to the person concerned, unless a lawful exception applies.

Being a family member or emergency contact does not automatically give someone authority to consent, make decisions or access records on another person's behalf.

7. Why we use personal information

We use personal information where necessary to:

- Respond to enquiries and arrange membership or services.
- Provide safe, suitable and person-centred activities.
- Understand communication, health and support needs.
- Manage attendance, transport and emergency arrangements.
- Communicate with members, families, carers and representatives.
- Identify and respond to safeguarding concerns.
- Recruit, support and manage staff and volunteers.
- Administer payments, donations, Gift Aid, payroll, pensions and expenses.
- Arrange training and maintain necessary records.
- Handle accidents, incidents, complaints and insurance matters.
- Meet legal, regulatory, accounting and governance responsibilities.
- Assess and improve services, using anonymised information where practicable.

We will explain where information is required for a service or legal obligation and the consequences of not providing it. Where missing information prevents safe support, we will discuss suitable arrangements with the individual or their authorised representative.

8. Our lawful bases for using information

We must identify and record an appropriate lawful basis before using personal information.

Depending on the purpose, this may include:

- Consent, where an individual has a genuine choice, such as permission for publicity photographs.
- Contract, where processing is necessary to enter into or perform a contract with the individual.
- Legal obligation, where processing is necessary to meet an applicable legal duty.
- Vital interests, where processing is necessary to protect someone's life.
- Legitimate interests, where processing is necessary for a legitimate purpose and is balanced against the individual's rights and interests.

Our legitimate interests may include organising services, maintaining safe operations, administering donations, preventing fraud and handling appropriate enquiries.

A volunteer arrangement, insurance requirement or safeguarding concern does not automatically establish a particular lawful basis. The circumstances must be assessed.

We will provide further information about the basis used for a particular activity on request.

9. Health and other sensitive information

Health and dementia-related information is special category personal data.

To use this information, we must identify both an Article 6 lawful basis and an applicable Article 9 condition, together with any additional safeguards required by UK law.

Depending on the circumstances, the condition may concern explicit consent, employment obligations, health or social care, legal claims, vital interests or a qualifying substantial public interest purpose such as safeguarding.

These conditions have specific requirements. We must not assume they apply simply because we support people living with dementia. Where required, we must maintain an appropriate policy document and meet relevant confidentiality obligations.

Criminal offence information, including relevant recruitment or safeguarding records, requires its own lawful authority and safeguards.

10. Consent, capacity and representatives

Where we rely on consent, it must be freely given, specific, informed and recorded. People must be able to withdraw consent easily.

Attendance at a session, submission of a form, employment, volunteering or making a donation does not automatically constitute consent to unrelated uses of information.

We support people to understand information and make their own decisions wherever possible. A diagnosis of dementia does not, by itself, mean that someone lacks capacity.

Where a representative acts for an individual, we must check their authority and the scope of the decisions they can make. We must not assume that a relative can give consent on someone else's behalf.

Where consent cannot validly be obtained, any proposed processing must have another applicable lawful basis and, where relevant, a special category condition.

Consent arrangements must be reviewed where the person's wishes, capacity, circumstances or representative arrangements change.

Withdrawing consent does not affect earlier lawful processing. We will explain if specific records must be retained under a separate legal requirement.

11. Photographs, videos and publicity

We may ask adults attending sessions, staff, volunteers and people involved in sessions arranged with partner organisations for permission to use identifiable photographs, videos or personal stories in publications, printed materials, fundraising, websites and social media.

Our existing publicity arrangements concern participants aged 18 and over. Images or information identifying children must not be used under those arrangements without a separate, appropriate assessment and permission process.

The permission request must explain the intended use and where the material may appear. Permission must be recorded clearly.

People must not be pressured to take part. Refusing publicity permission must not, by itself, affect access to ordinary services.

Staff must consider dignity, distress, capacity and the person's expressed wishes. A relative's agreement must not override an individual's valid refusal.

People can contact us to withdraw permission. We will stop future use where consent is withdrawn and take reasonable steps concerning material under our control. We will explain any practical limits involving material already printed, distributed or republished by others.

12. Sharing personal information

We share personal information only where there is a lawful, necessary and proportionate reason.

Depending on the circumstances, recipients may include:

- Emergency services.
- Health and social care professionals.
- Local authorities and safeguarding teams.
- Approved transport providers and authorised drivers.
- Training, payroll, pension and employee benefit providers.
- HMRC and other relevant public authorities.
- Payment providers, including GoCardless where used.
- Insurers, auditors, regulators, funders and professional advisers.
- Approved IT, hosting, storage and form providers.

Only the information necessary for the purpose may be shared. The recipient, authority and secure method must be checked.

Significant or sensitive sharing decisions must be recorded where appropriate. Where anonymised information meets a funder's or partner's needs, identifiable records must not be supplied unnecessarily.

13. Sharing between the CIC, CIO and volunteers

The CIC shares relevant Jotform information and Gift Aid records with authorised CIO personnel only as and when necessary to collect, reconcile and administer donations and Gift Aid.

This may include a member identifier, donor name and contact details, donation amounts, payment status, Gift Aid declarations and relevant supporting records.

Donation administration must not give the CIO unrestricted access to complete member submissions, detailed health records or unrelated care information.

Authorised charity volunteers may receive only the member details necessary for their assigned duties and safe support. For example, a driver may need collection details and essential mobility or safety instructions. A limited extract must be used where it will meet the need instead of a full member record.

Volunteers must follow the CIC's secure handling instructions. They must not forward information to unauthorised people, retain it for personal use or use it for another purpose. They must return or securely delete it when no longer required.

The organisations must document sharing arrangements, including the purpose, permitted information, lawful basis, responsibilities, security and retention requirements. Any information revealing or allowing an inference about health requires appropriate additional protection.

14. Jotform and online forms

Dementia Active CIC uses Jotform for relevant online forms. The CIC is the controller for the forms it operates. Jotform provides the platform and processes submissions on the CIC's behalf.

Jotform may have separate responsibilities for information it uses for its own purposes, such as account administration and website operation.

Forms must request only necessary information, explain their purpose and link to relevant privacy information. Submitting a form does not automatically establish valid consent.

Access to submissions must be restricted to authorised CIC staff who need the information for their duties, subject to the limited sharing and provider processing described in this policy. Complete submissions, attachments, reports and tables must not be made generally accessible to the CIO or volunteers.

Managers must approve access, review it regularly and remove it promptly when duties change or a person leaves. Moving from the CIC to the CIO does not create a continuing right to CIC records.

Staff must:

- Use individual authorised accounts wherever available, strong passwords and multi-factor authentication wherever supported.
- Keep submissions, reports and attachments protected from public access.
- Exclude sensitive answers from routine email notifications wherever practicable and access the protected record instead.
- Protect downloads, exports, printouts and approved extracts.
- Check recipients and sharing permissions.
- Report lost information, misdirected messages and suspected breaches immediately.

New integrations, automated forwarding, AI features or external access must undergo a documented privacy and security review before management authorisation.

15. Service providers and overseas processing

Approved providers may process information to supply hosting, security, maintenance, payment processing, communications and technical support.

Before using a provider, the responsible organisation must assess its suitability and put appropriate contractual arrangements in place where required.

The CIC must retain an applicable Data Processing Addendum with Jotform and assess relevant subprocessors and features. Provider access needed for hosting, security, maintenance and support is

separate from access by CIC staff and the limited CIO sharing described above.

Jotform is based in the United States and offers different storage arrangements. The CIC must establish and document the actual storage region, relevant subprocessors and overseas access arrangements applying to its account.

UK or European storage does not necessarily prevent access from another country or legally required disclosure.

Where a restricted international transfer occurs, the responsible organisation must establish an appropriate legal transfer mechanism and complete any required transfer risk assessment or data protection test, with additional safeguards where necessary. Where contractual safeguards are used, the applicable UK arrangements, such as the UK Addendum to Standard Contractual Clauses or the International Data Transfer Agreement, must be checked as appropriate.

A provider's general compliance statement or overseas location does not, by itself, establish that the organisation's transfer obligations have been met.

Individuals may contact us for information about relevant overseas processing and safeguards, including how to obtain information about applicable transfer arrangements.

Providers may also have to respond to valid legal demands. We do not promise that information can never be accessed outside Dementia Active.

16. Staff, volunteer and applicant information

The organisation employing or engaging an individual uses relevant information to manage recruitment, employment or volunteering, support wellbeing, provide training, make payments and meet legal duties.

Records may include:

- Applications, references, qualifications and suitability checks.
- Role, contract, start date and leaving date.
- Working patterns, timesheets, attendance, training and performance.
- Salary, overtime, bank details, tax status, payroll, pensions and expenses.
- Annual leave and sickness absence.
- Maternity, paternity, shared parental and adoption leave and pay.
- General health and wellbeing information, fit notes, occupational health referrals and reports, and workplace accident records.

The lawful basis depends on the purpose and may include contract, legal obligation, legitimate interests or consent where consent is appropriate. Health information also requires a suitable special category condition.

Consent must not be relied on where the individual does not have a genuine choice.

Information may be shared with authorised managers, training suppliers, payroll and pension providers, employee benefit schemes, HMRC, insurers, auditors and professional advisers where necessary and lawful.

17. Retention and secure disposal

We keep personal information only for as long as necessary for its purpose and applicable legal, safeguarding, insurance and governance requirements.

Our general retention approach is:

- Member registration records: retained while membership or support continues. Information is then deleted from Jotform unless limited records remain necessary for a justified legal, safeguarding, insurance, complaint or governance purpose.
- Health, emergency and support information: reviewed regularly and updated promptly; retained only while necessary, subject to applicable safeguarding, legal and insurance requirements.
- Accident, incident and complaint records: normally retained for at least three years, with longer retention where legal, safeguarding, insurance or unresolved matters justify it.
- Safeguarding records: retained according to the nature of the concern, relevant guidance and continuing risk.
- Staff and volunteer files: generally retained for up to six years after leaving, subject to justified exceptions.
- Financial, payroll and tax records: generally retained for six years where applicable, with different or longer periods where required for particular records, including pensions.
- Publicity permission records: retained while associated material is used and for any further period needed to demonstrate permission or address a dispute.
- Marketing contacts: retained while there is an appropriate basis for contact. A limited suppression record may be retained to respect an unsubscribe request.

These periods are not automatic deletion rules for every record. The responsible organisation must maintain a documented retention schedule, assign a period or clear criteria to each form and record type, and apply legal holds where necessary.

Deletion must cover relevant submissions, exports, attachments, notifications and copies shared with the CIO or volunteers. Backup and provider deletion arrangements must also be considered.

Paper records must be securely shredded or destroyed. Devices and storage media must be securely erased or destroyed before disposal or reuse.

18. Your data protection rights

Depending on the circumstances, you may have the right to:

- Receive information about how your personal information is used.
- Request access to your information.
- Ask for inaccurate or incomplete information to be corrected.
- Request deletion.
- Request restrictions on use.
- Object to certain processing.
- Receive and transfer certain information in a usable format.
- Withdraw consent where processing relies on consent.

- Exercise applicable rights concerning significant automated decisions.

These rights are subject to legal conditions and exceptions. Please use the contact details in section 4 to make a request or ask which rights apply.

19. Handling rights requests

Requests can be made verbally or in writing. A special form or legal terminology is not required.

Staff must pass requests promptly to Andrew Gill or the designated data protection lead.

We may make proportionate checks of identity and any representative's authority before disclosing information.

We respond without undue delay, normally within one calendar month. Where the law permits an extension or adjustment to the deadline, we will explain the reason and applicable timescale.

Requests are normally free. If a lawful exception permits a fee or refusal, we will explain the decision and available complaint routes.

20. Marketing, website information and cookies

Service messages, such as changes to sessions or transport, are separate from fundraising and promotional communications.

We must identify the appropriate lawful basis and meet applicable electronic marketing requirements before sending promotional messages. Where consent is required, we must obtain it.

People can ask us to stop direct marketing at any time. Relevant messages must provide an appropriate way to opt out.

Our website and embedded services may use cookies or similar technologies. Information about their purposes and available choices must be provided through the website's cookie information and controls.

Where consent is required, the relevant technology must not be used before valid consent has been obtained. Continuing to browse does not, by itself, provide consent.

Links to other websites are subject to those organisations' privacy arrangements.

21. Confidentiality and secure handling

Personal and confidential information must be accessed only by authorised people who need it for their role.

Staff, volunteers, trustees, directors and contractors must:

- Keep information confidential during and after their involvement with Dementia Active.
- Use approved accounts, systems and storage.
- Check recipients and attachments before sending information.
- Use an appropriate secure method for sensitive records.
- Keep paper records in locked or otherwise appropriately secured storage.
- Avoid unnecessary copies and printing.

- Lock unattended devices and protect screens from view.
- Avoid confidential conversations where they can be overheard.
- Follow retention and disposal requirements.
- Ask for guidance if unsure whether information can be used or shared.

Confidential records must not be placed in unapproved personal email, messaging, cloud storage or AI services.

Information must not be discussed with friends, relatives or other unauthorised people, or posted on personal social media.

22. Cyber security safeguards

Dementia Active must maintain security measures appropriate to the information held and risks to individuals.

Required measures include:

- Strong, unique passwords and confidential login details.
- Individual accounts wherever supported.
- Multi-factor authentication wherever available.
- Restricted administrator access.
- Regular access reviews and prompt removal of unnecessary access.
- Supported software and timely security updates.
- Appropriate malware protection and firewalls.
- Encryption on portable devices holding personal information.
- Secure backups protected from unauthorised alteration or deletion, and periodic restoration checks.
- Assessment of external providers and new systems.
- Appropriate staff and volunteer guidance.

These requirements cover approved systems including Jotform, Road Link and other transport planning systems, email, cloud storage, websites and financial systems.

Where a required safeguard is unavailable, the CEO must arrange a risk assessment and suitable alternative controls.

Requests for unusual payments, changes to bank details or disclosure of sensitive information must be verified through a separate, trusted contact method.

23. Working away from premises

When travelling, working at home or delivering community sessions, personnel must carry or access only the information needed.

Paperwork and devices must be kept secure and must not be left visible in vehicles or public places. Records must be returned to secure storage promptly.

Personal devices may be used only with authorisation and suitable safeguards. Organisational information must not be accessible to household members or copied automatically to unapproved

personal accounts.

Remote access must use approved methods. Suspected loss or theft must be reported immediately.

24. Safeguarding and information sharing

Confidentiality must not prevent appropriate action to protect someone from abuse, neglect or serious harm.

Concerns must be reported immediately under Dementia Active's Safeguarding Policy.

Information may be shared with appropriate professionals or authorities where necessary, proportionate and lawful. Only relevant information should be disclosed.

Staff must record the reason, recipient and lawful basis for significant disclosures and seek management guidance where practicable. Urgent protective action must not be delayed by routine internal approval processes.

25. Recognising and reporting security incidents

A security incident or personal data breach may involve:

- Information sent to the wrong person.
- Lost paperwork, devices or emergency contact records.
- Unauthorised access to an account or record.
- Phishing, malware, ransomware or fraudulent instructions.
- Publicly accessible submissions, reports or shared folders.
- Accidental deletion or alteration.
- Inappropriate verbal disclosure.
- Unexplained changes to transport, member or financial records.
- Loss of access to information needed to operate safely.

All suspected incidents must be reported immediately to the CEO, designated deputy or responsible manager, even where the facts are uncertain.

Staff must not wait to complete a form or obtain proof. If email may be compromised, use a trusted alternative communication route.

26. Cyber attack and breach response

The CEO or nominated incident lead must coordinate the response.

The immediate priorities are to:

1. Protect members, including transport, attendance, essential support and safeguarding arrangements.
2. Escalate the incident and obtain appropriate technical assistance.
3. Contain the problem, including disconnecting affected devices from networks where safe and appropriate.
4. Preserve evidence and record the timeline.

5. Secure compromised accounts from a trusted device, including resetting passwords and revoking sessions where appropriate.
6. Assess affected information, systems, organisations and people, including whether information has been accessed, altered, lost or made unavailable.
7. Make required notifications and communicate necessary protective advice.
8. Restore services only after appropriate checks and authorisation.

Staff must not delete evidence, wipe devices, attempt unauthorised repairs, contact attackers, negotiate or make ransom payments.

Extortion demands must be escalated immediately for specialist advice.

27. Breach assessment and notifications

The responsible organisation must assess the likelihood and severity of harm, considering the information involved, the people affected and their vulnerability.

Where a personal data breach is likely to result in a risk to people's rights and freedoms, the responsible controller must notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it.

Where a breach is likely to result in a high risk, affected individuals must also be informed without undue delay, subject to applicable legal exceptions.

Incomplete information must not prevent an initial notification where required. Further information can be supplied in stages.

All personal data breaches must be recorded, including the reasons for decisions not to notify.

Trustees must separately assess Charity Commission serious incident reporting requirements where the charity is affected. Safeguarding, police, insurance and contractual notifications must also be considered where relevant.

28. Member safety, transport and business continuity

Member safety takes priority over administrative recovery.

Each centre must have an approved, secure way to access essential information during a system outage. This must contain only what is necessary, such as attendance, emergency contacts, essential support information and transport arrangements.

Emergency records must be accurate, accessible to authorised staff and protected from unauthorised use. Superseded copies must be securely destroyed.

Potentially compromised collection instructions, contact details or care information must be verified through trusted sources before use.

Activities must be adapted or suspended where missing or unreliable information creates an unacceptable risk.

Temporary records must be kept securely and reconciled after recovery. Affected families, carers and providers must receive necessary operational updates.

Where there is immediate danger, staff must contact emergency services as necessary and activate relevant safeguarding procedures.

29. Recovery, incident records and communications

Before affected systems return to use, Dementia Active must check that the cause has been addressed, access is secure and critical records are accurate.

Recovery may include restoration from trusted backups, verification of transport and member records, reconciliation of temporary records and monitoring for continuing problems.

The CEO must coordinate operational approval with Centre Managers and relevant technical support.

A restricted incident register must record:

- Discovery and reporting times.
- Affected systems, information and organisations.
- Actual or potential harm.
- Immediate safety and containment measures.
- Risk assessments and notification decisions, including reasons.
- Communications and recovery actions.
- Lessons, action owners and completion dates.
- Authorisation to restore services and close the incident.

The CEO or nominated representative must coordinate external communications. Messages must be accurate, accessible and limited to necessary information. Staff must distinguish confirmed facts from matters under investigation and must not speculate or make unauthorised public statements.

30. Responsibilities, training and oversight

The CEO oversees implementation, appoints appropriate leads and deputies, coordinates serious incidents and ensures significant concerns reach the relevant governing body. Incident reporting must not depend on one person being available.

Trustees and CIC directors provide oversight for their respective organisations and ensure appropriate controls and resources.

Centre Managers maintain safe operational arrangements, secure emergency information and contingency procedures.

The designated data protection lead supports privacy notices, rights requests, breach assessment, retention, staff guidance and privacy enquiries.

Staff, volunteers and contractors must read and follow this policy, protect information, complete relevant training and report concerns immediately.

IT and system providers support security, investigation and restoration within their agreed responsibilities.

Relevant personnel must receive induction guidance and refresher training. Training must cover confidentiality, safe sharing, phishing, account security, safeguarding and incident reporting.

Significant incidents and realistic outage scenarios must be reviewed or practised to identify improvements. The CEO must ensure lessons are assigned to named action owners and followed through.

31. Privacy complaints and the ICO

If you are concerned about how we have handled personal information, please contact us using the details in section 4.

Complaints may be made by email, telephone, post or an available complaints form. Using a form is not compulsory.

We will acknowledge a data protection complaint within 30 days, investigate without undue delay, keep the complainant appropriately informed and communicate the outcome.

You also have the right to complain to the Information Commissioner's Office.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113

Website: https://ico.org.uk/make-a-complaint/

32. Policy review, document control and approval

This policy must be reviewed at least annually and sooner following:

- A significant cyber incident or personal data breach.
- A safeguarding issue involving information.
- A significant privacy complaint.
- Changes to services, staffing, systems, providers, Jotform features, subprocessors or sharing arrangements.
- Relevant changes to law or regulatory guidance.

Website notices, forms, staff and volunteer privacy information and related policies must remain consistent with the organisation's actual arrangements and this policy.

The existing policy records Andrew Gill, 8 June 2026, approval by the Trustees, and a review date of 7 June 2027. These historical details are retained; they do not establish approval of this consolidated version or approval by the CIC directors.

The website wording changes dated 12 October 2026 clarified data protection complaints, CIC controller status and information sharing. They did not replace the existing approval record or confirm a review of operational data arrangements.

The consolidated rewrite dated 25 October 2026 incorporates those changes and cyber security requirements. The CEO must arrange approval through the appropriate CIO and CIC governance procedures and maintain a record of the version approved, approving body, approval date and next review date.

Until a newly approved review schedule is recorded, the existing scheduled review date remains 7 June 2027. Earlier review is required where a significant change or incident makes it necessary.