Focusing on Ability

DEMENTIA ACTIVE

Cyber Security and Cyber Attack Response Policy

Policy and operational response arrangements

Document control	Details
Applies to	Dementia Active Charity and Dementia Active Community Interest Company
Charity number	1195246
CIC registration number	11973554
Policy date	21 October 2026
Version	1.0
Policy owner	Chief Executive Officer
Approval	Board of Trustees / CIC Directors, for their respective organisations
Review frequency	Annually, and following a significant incident or material change
Next review	20 October 2027
Related documents	Privacy Policy, Safeguarding Policy, Data Retention arrangements and Business Continuity Plan

Dementia Active Charity | Dementia Active Community Interest Company

1. Purpose

Dementia Active is committed to protecting the personal, confidential and sensitive information entrusted to us by members, their families and carers, staff, volunteers, donors and professional partners.

As an organisation supporting people living with dementia, we recognise that a cyber attack or data breach could affect people's safety, dignity and wellbeing. Particular risks arise where information concerns health, safeguarding, home addresses, transport arrangements or emergency contacts.

This policy establishes requirements for preventing, identifying, reporting, responding to and recovering from cyber security incidents. Its priorities are to:

- Protect members and maintain safe services.
- Prevent unauthorised access, disclosure, alteration or loss of information.
- Maintain accurate and available records.
- Meet applicable data protection and reporting obligations.
- Learn from incidents and improve security.

2. Scope

This policy applies to employees, trustees, directors, volunteers, temporary workers and authorised contractors working on behalf of either organisation.

It covers information held or processed through:

- Jotform, including referrals, assessments and incident reports.
- Road Link and other transport planning systems.
- Email, cloud storage and shared documents.
- Computers, mobile phones, tablets and removable storage.
- Financial, payroll and donation systems.
- Websites, online forms and external service providers.
- Paper records used during an outage or otherwise affected by a cyber incident.

It applies at centres, in vehicles, at home and wherever organisational information is accessed.

3. Responsibilities

Role	Responsibility
CEO	Lead the response, appoint an incident lead, arrange specialist support, coordinate recovery and escalate serious incidents.
Trustees and CIC Directors	Oversee risks, resources and controls; approve the policy for their organisation and ensure relevant reporting obligations are addressed.
Centre Managers	Protect members, maintain secure emergency information, implement contingency arrangements and report incidents.
Designated data protection lead	Support breach assessment, maintain records and coordinate required notifications.
Staff and volunteers	Follow security requirements, attend relevant training and report concerns immediately.
IT and system providers	Provide technical support for prevention, containment, investigation and safe restoration within agreed responsibilities.

The CEO must nominate a deputy who can act when the CEO is unavailable. Incident reporting must not depend on one person being available.

4. Information ownership and sharing between organisations

The charity and CIC must identify their respective responsibilities for the personal information they collect and use. Sharing a name, staff or systems does not automatically permit unrestricted access between the organisations.

For each significant processing activity, the responsible organisation must establish:

- Which organisation determines why and how information is used.
- Whether the organisations act as separate controllers, joint controllers or controller and processor.
- The lawful basis for processing and, where relevant, the additional condition for using health or other special category information.
- Which staff require access and what information they need.
- Any necessary data sharing, joint controller or processing agreements.
- How these arrangements are explained in the Privacy Policy.

Access must be separated through permissions, accounts or other suitable controls where appropriate. Unnecessary duplication of sensitive records must be avoided.

5. Access and account security

Access must be limited to the information and functions needed for each person’s responsibilities.

Dementia Active requires:

- Individual accounts wherever supported, with no sharing of personal login credentials.
- Strong, unique passwords and an approved password manager where appropriate.
- Multi-factor authentication wherever available, prioritising email, sensitive systems and administrator accounts.
- Separate administrator access where practicable, used only for administrative tasks.
- Regular access reviews and prompt changes when responsibilities change.
- Prompt withdrawal of access when someone leaves or no longer requires it.
- Screens to be locked when unattended.

Where a system cannot support a required safeguard, the CEO must arrange a risk assessment and suitable alternative controls.

6. Device, software and network security

Devices used for work must have appropriate access protection, supported software and timely security updates. Malware protection and firewalls must be enabled where appropriate.

Portable devices containing personal information must use encryption. Lost or stolen devices must be reported immediately so that access can be blocked and remote locking or erasure considered where available.

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

Staff must not install unapproved software or disable security controls. Remote access must use approved methods, and sensitive information must not be accessed where others can see or overhear it.

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

7. Safe handling and communication

Personal information must be collected, accessed and shared only where necessary for an authorised purpose.

Staff and volunteers must:

- Use approved storage, email and communication services.
- Check recipients, attachments and sharing permissions before sending information.
- Use an approved secure method for sensitive records.
- Avoid revealing recipients' details in group communications.
- Verify unexpected requests for confidential information through a separate, trusted contact method.
- Keep paper records secure and retrieve printouts promptly.
- Follow retention requirements and securely dispose of records when no longer needed.

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

Requests to change bank details or make unusual payments must be independently verified using established contact details and the organisation's financial approval procedures.

8. Backups and emergency information

Essential records must be backed up securely at a frequency appropriate to the risk and the amount of information that could safely be lost.

Backups must be protected against unauthorised access and against being altered or deleted through a compromised everyday account. Restoration must be tested periodically, with results and corrective actions recorded.

Each centre must maintain an approved, secure means of accessing essential information during a system outage. This must contain only what is necessary for safe operation, such as:

- Current attendance and transport arrangements.
- Emergency contact details.
- Essential health, communication and support information.
- Relevant safeguarding instructions.

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

9. External systems and service providers

Before a provider is allowed to handle personal information, Dementia Active must assess whether its security and data protection arrangements are suitable.

Reviews must consider access controls, hosting arrangements, incident reporting, backups, recovery, data export and secure deletion. Appropriate written agreements must be in place where required.

A maintained provider list must include the service owner, support details, information held and emergency escalation route. Any overseas processing must be assessed against applicable data protection requirements.

Using an external provider does not remove Dementia Active's responsibility to understand and manage the risks.

10. Recognising and reporting incidents

An incident may include:

- Unauthorised access to information or accounts.
- Phishing, fraudulent payment requests or stolen passwords.
- A lost or stolen device or paper emergency pack.
- Ransomware, malware or unexplained file changes.
- Compromised email, Jotform, Road Link or cloud accounts.
- Information sent to the wrong recipient.
- Publicly accessible forms, folders or sharing links containing personal information.

- Unexplained changes to referral, transport or financial records.
- A system failure that prevents safe access to essential information.

All suspected incidents must be reported immediately, even where the facts are uncertain. Staff must not wait to complete a form or obtain proof.

Reports must go to the CEO or designated deputy using a trusted communication route. If email may be compromised, use a known telephone number or another approved channel.

11. Immediate cyber attack response

The incident lead must coordinate the following actions.

1. Protect members. Check attendance, transport, emergency contacts, safeguarding and essential support arrangements.
2. Escalate. Inform the CEO or deputy and obtain appropriate technical assistance.
3. Contain. Where safe and appropriate, disconnect affected devices from Wi-Fi or wired networks. Follow technical advice on further action.
4. Preserve evidence. Record times, warning messages and actions taken. Do not delete files, wipe devices or attempt an unauthorised investigation.
5. Secure accounts. From a trusted device, arrange password resets, revoke compromised sessions and review access and account settings.
6. Assess the impact. Establish which organisations, systems, records and people are affected, and whether information has been accessed, changed, lost or made unavailable.
7. Consider notifications. Assess regulatory, safeguarding, contractual, insurance and law enforcement reporting requirements.
8. Recover safely. Restore services only after appropriate checks and authorisation.

Staff must not contact attackers, negotiate or make ransom payments. Any extortion demand must be escalated immediately to the CEO for specialist advice.

12. Protection of members and continuity of services

Member safety takes priority over administrative recovery.

Where transport systems or member databases are unavailable or potentially inaccurate, Centre Managers must use approved contingency information and verify critical details through trusted sources.

Staff must not rely on potentially compromised collection instructions, emergency contacts or care information until their accuracy has been checked. Temporary records must be securely held and reconciled with the main system after recovery.

Where an incident creates a safeguarding concern, safeguarding procedures must be activated alongside the cyber response. Immediate danger must be addressed through emergency services where necessary.

An activity must be suspended or adapted where missing or unreliable information creates an unacceptable risk. Necessary changes must be communicated promptly to affected families, carers and transport providers.

13. Personal data breaches and reporting

Dementia Active will assess personal data breaches under applicable UK data protection law, including the UK GDPR and Data Protection Act 2018, as amended.

The assessment must consider the sensitivity of the information, the people affected, their vulnerability, possible consequences and the effectiveness of protective measures.

Where required, the responsible controller must notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Incomplete information must not prevent an initial notification where one is required; further information may be supplied in stages.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals must be informed without undue delay, subject to applicable legal exceptions. Communications must explain what happened, likely consequences, action taken, protective steps and a contact for assistance.

All personal data breaches must be documented, including decisions not to notify. These requirements follow the ICO's breach guidance.

For incidents affecting the charity, trustees must assess whether a serious incident report to the Charity Commission is required and ensure prompt reporting where appropriate. This is separate from ICO reporting. See the Charity Commission's serious incident guidance.

14. Communications

The CEO or nominated representative must coordinate communications with members, families, staff, providers and external bodies.

Messages must be accurate, accessible and limited to necessary information. Where relevant and lawful, communication should involve an authorised representative, taking account of the individual's needs and preferences.

Staff must not speculate, disclose confidential incident details or issue public statements without authorisation. Updates must distinguish confirmed facts from matters still under investigation.

15. Recovery and return to service

Recovery must include:

- Checking that the cause has been contained or addressed.
- Restoring from trusted sources where required.
- Verifying the accuracy of critical member, transport and financial records.
- Checking access permissions and account security.
- Reconciling temporary records.
- Confirming that essential services can operate safely.
- Recording authorisation to return affected systems to use.

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

16. Incident register and learning

Every suspected attack, personal data breach and significant system failure must be recorded in a restricted incident register.

Records must include the timeline, affected systems, member safety implications, containment actions, risk assessment, notification decisions, recovery and lessons learned.

Following a significant incident, the CEO must arrange a review, assign improvement actions and report material findings to the relevant trustees or directors. Records must be retained under an approved retention schedule.

17. Training, review and approval

Staff and volunteers must receive guidance appropriate to their role at induction and through refresher training. Topics must include phishing, passwords, safe sharing, incident reporting and outage procedures.

Relevant staff must periodically practise the response to a realistic scenario, including loss of transport records or a compromised email account.

This policy must be reviewed annually and after a significant incident, major system change or relevant change in requirements.

18. Contact and escalation

CEO: Andrew Gill

Telephone: 01869 713 913

Email: dementiactive@gmail.com

Designated deputy and telephone: [insert]

IT support and emergency telephone: [insert]

Safeguarding lead and telephone: [insert]

If an account or communication channel may be compromised, use a separately verified alternative.

Appendix A - Cyber incident report form

Part 1 of 2 - Initial report and immediate action

Report immediately by telephone or another trusted route before completing this form. Store completed forms securely.

Field	Details to record
Incident reference	
Reporter, role and safe contact number	
Centre and organisation affected	Charity / CIC / both
Date and time discovered	
Date and time reported; reported to whom	
What happened?	Record facts and identify uncertainties.
Systems, accounts or devices affected	
Information potentially affected	Categories and approximate volume; avoid unnecessary personal details.
People potentially affected	Approximate numbers and relevant vulnerabilities.
Immediate member safety or safeguarding risk	

Appendix A - Cyber incident report form

Part 2 of 2 - Assessment, reporting and recovery

Report immediately by telephone or another trusted route before completing this form. Store completed forms securely.

Incident reference: _____

Field	Details to record
Containment and continuity actions	Include who acted and when.
Evidence location	Secure reference to relevant logs, messages or screenshots.
Incident lead and technical support	
Personal data breach assessment	Risk, reasoning and time the controller became aware.
ICO decision	Notify / do not notify / assessment ongoing; reasons, deadline and reference.
Affected individuals	Notification decision, reasons, date and communication method.
Other reporting	Charity Commission, safeguarding bodies, police, insurer or contractual contacts.
Recovery and verification	Checks completed and authorisation to restore service.
Lessons and outstanding actions	Owner and target date for each action.
Closure	Approved by and date.

Appendix B - Centre emergency action sheet

CYBER INCIDENT: PROTECT MEMBERS - REPORT - CONTAIN - RECORD

1. Make members safe. Check attendance, transport, essential support and safeguarding.

2. Contact the CEO or deputy immediately. Use a known telephone number if email is suspicious.

3. Stop using affected systems. Disconnect a suspected infected device from the network where safe; seek technical advice.

4. Preserve evidence. Record what you saw and when. Do not delete, wipe or attempt repairs.

5. Use approved emergency records. Verify transport instructions and critical contacts before relying on them.

6. Follow the incident lead's instructions. Do not contact attackers or make public statements.

7. Keep a secure action log. Record decisions, temporary arrangements and communications.

8. Resume only when authorised. Confirm records and systems are safe and accurate.

CEO: 01869 713 913

Deputy: [insert]

IT support: [insert]

Safeguarding lead: [insert]

Emergency services: 999 where there is immediate danger.

Complete and verify these contacts before issuing the sheet to centres.

Appendix C - Suggested addition to the public Privacy Policy

Publish once the arrangements described have been confirmed.

Keeping your information secure

Dementia Active takes appropriate technical and organisational measures to protect personal information against unauthorised access, misuse, accidental loss, alteration or disclosure.

These measures include access restrictions, account and device security, staff guidance, secure information sharing, backups and incident response arrangements. We apply particular care to health, safeguarding and other sensitive information.

Dementia Active Charity and Dementia Active CIC manage access according to their respective responsibilities. Information is shared between them only where necessary, lawful and appropriately protected.

If a security incident affects personal information, we will investigate, take steps to reduce harm and notify the relevant regulator and affected individuals where legally required.

To raise a privacy or security concern, contact dementiactive@gmail.com or 01869 713 913.