ANCHOREACH C.I.C.

GDPR and Data Protection Policy and Procedures

Policy Owner: Anchoreach C.I.C.
Approved by: Board of Directors
Date Approved:17/08/2026
Review Date: 17/08/2027
Version: 1.0

---

1. Policy Statement

Anchoreach C.I.C. is committed to protecting the privacy, confidentiality and security of personal information entrusted to us.

We recognise that people have a right to know how their personal information is collected, used, stored and shared.

Anchoreach C.I.C. will comply with applicable UK data protection legislation, including the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

We will ensure that personal information is handled lawfully, fairly, transparently and securely.

---

2. Purpose

This policy sets out how Anchoreach C.I.C. will:

- Collect and use personal information responsibly.
- Protect personal information from unauthorised access, loss, misuse or disclosure.
- Ensure compliance with UK GDPR and the Data Protection Act 2018.
- Respect individuals' data protection rights.
- Ensure staff, directors and volunteers understand their responsibilities.
- Respond appropriately to data protection incidents and breaches.
- Maintain appropriate records and procedures.

---

3. Scope

This policy applies to:

- Directors.
- Employees.
- Volunteers.
- Freelancers and sessional workers.

- Tutors and facilitators.
- Contractors.
- Students and participants.
- Anyone else handling personal information on behalf of Anchoreach C.I.C.

It applies to personal information held in:

- Paper records.
- Computers.
- Laptops and tablets.
- Email accounts.
- Cloud storage.
- Databases.
- Online forms.
- Mobile devices.
- Photographs and videos.
- Other electronic or physical records.

---

4. What Is Personal Data?

Personal data is information relating to an identified or identifiable living individual.

Examples may include:

- Name.
- Address.
- Telephone number.
- Email address.
- Date of birth.
- Emergency contact details.
- Attendance records.
- Training records.
- Qualifications.
- Employment information.
- Images and photographs.
- CCTV footage.
- IP addresses or online identifiers.
- Information contained within case notes.
- Information relating to support provided.

Some information is considered **special category data** and requires additional protection.

This may include information relating to:

- Health.
- Disability.
- Race or ethnic origin.
- Religion or beliefs.
- Sexual orientation.
- Genetic or biometric information where used for identification.

Anchoreach C.I.C. will only collect special category data where there is a lawful and appropriate reason to do so.

---

5. Data Protection Principles

Anchoreach C.I.C. will comply with the core UK GDPR principles.

Personal data must be:

1. Lawful, fair and transparent

We will have a valid legal basis for processing personal data and explain clearly how information is used.

2. Purpose limited

Information will only be collected and used for specified, explicit and legitimate purposes.

3. Adequate, relevant and limited

We will only collect information that is necessary for the purpose.

4. Accurate

We will take reasonable steps to keep information accurate and up to date.

5. Stored appropriately

Information will not be kept for longer than necessary.

6. Secure

Appropriate technical and organisational measures will be used to protect information.

---

6. Lawful Basis for Processing

Before collecting or using personal data, Anchoreach C.I.C. will identify an appropriate lawful basis.

Depending on the circumstances, this may include:

- Consent.
- Contract.
- Legal obligation.
- Vital interests.
- Public task.
- Legitimate interests.

Consent will only be relied upon where it is appropriate and will be obtained through a clear and positive action.

Individuals will be informed about how their information will be used.

---

7. Consent

Where consent is required, Anchoreach C.I.C. will ensure that consent is:

- Freely given.
- Specific.
- Informed.
- Unambiguous.
- Clearly recorded.

Individuals will be able to withdraw consent where consent is the lawful basis for processing.

Withdrawal of consent will not affect processing that was lawfully carried out before consent was withdrawn.

---

8. Privacy Information

Where personal data is collected, Anchoreach C.I.C. will provide appropriate privacy information explaining:

- Who is collecting the information.

- What information is being collected.
- Why it is being collected.
- How it will be used.
- The lawful basis for processing.
- Who it may be shared with.
- How long it will be retained.
- The individual's data protection rights.
- How to contact Anchoreach C.I.C. about their information.

---

9. Data Collection

Anchoreach C.I.C. will only collect personal information that is necessary for legitimate organisational purposes.

Information may be collected through:

- Registration forms.
- Enrolment forms.
- Referral forms.
- Attendance registers.
- Feedback forms.
- Surveys.
- Email.
- Telephone.
- Website forms.
- Funding monitoring requirements.
- Volunteer applications.
- Employment applications.
- Training records.
- Photographs and videos.

Staff must not collect unnecessary personal information.

---

10. Children and Young People

Where Anchoreach C.I.C. works with children or young people, additional care will be taken with their personal information.

We will:

- Collect only information that is necessary.
- Use appropriate consent and lawful processing arrangements.
- Provide age-appropriate privacy information where appropriate.
- Keep children's information secure.
- Only share information where there is a legitimate and lawful reason.
- Follow safeguarding procedures where concerns arise.

Safeguarding responsibilities take priority where information needs to be shared to protect a child or young person from harm.

---

11. Confidentiality

Staff, directors and volunteers must treat personal information as confidential.

Personal information must not be:

- Discussed unnecessarily with others.
- Left unattended in public areas.
- Shared through personal social media accounts.
- Sent to unauthorised recipients.
- Stored on unauthorised personal devices.
- Used for purposes unrelated to the reason it was collected.

Confidential information should only be accessed by individuals who need it to carry out their role.

---

12. Information Security

Anchoreach C.I.C. will take reasonable and appropriate steps to protect personal information.

This may include:

- Password-protected devices.
- Strong passwords.
- Multi-factor authentication where available.
- Secure cloud storage.
- Access controls.
- Locked filing cabinets.

- Secure disposal of documents.
- Antivirus and security software.
- Regular software updates.
- Staff awareness and training.
- Secure email practices.

Personal data should not be stored on unapproved USB drives or personal cloud accounts.

---

13. Password Security

Staff and volunteers must:

- Use strong passwords.
- Keep passwords confidential.
- Never share passwords with other people.
- Avoid using the same password for multiple important accounts.
- Use multi-factor authentication where available.
- Lock devices when unattended.
- Report suspected compromised passwords immediately.

---

14. Email and Electronic Communication

When sending personal information by email, staff should check:

- The correct recipient has been selected.
- Attachments contain only necessary information.
- Sensitive information is appropriately protected.
- Emails are not being sent to unauthorised recipients.
- Group emails use appropriate privacy settings where required.

Where sensitive personal information is being sent electronically, appropriate security measures should be considered.

---

15. Paper Records

Paper records containing personal information must be stored securely.

Where appropriate:

- Files should be kept in locked cabinets.
- Documents should not be left unattended.
- Confidential paperwork should not be left in public areas.
- Visitors should not have unsupervised access to confidential records.
- Documents should be securely destroyed when no longer required.

---

16. Photographs and Videos

Photographs and videos may constitute personal data.

Before using photographs or videos for promotional, publicity or social media purposes, Anchoreach C.I.C. will ensure that an appropriate lawful basis exists.

Where consent is used, individuals will be informed about how their image will be used.

Additional care will be taken when photographing children and young people.

Individuals should not be tagged or identified unnecessarily in social media posts.

---

17. Sharing Personal Information

Anchoreach C.I.C. will only share personal information where there is a lawful basis for doing so.

Information may be shared with appropriate organisations such as:

- Funding bodies.
- Awarding organisations.
- Partner organisations.
- Safeguarding agencies.
- Local authorities.
- Emergency services.
- Professional advisers.
- Service providers processing information on our behalf.

Only information necessary for the specific purpose should be shared.

Where possible, anonymised or aggregated information should be used for reporting.

---

18. Data Processors and Third Parties

Where an external organisation processes personal information on behalf of Anchoreach C.I.C., appropriate checks will be undertaken.

Where required, a written data processing agreement or appropriate contractual terms will be used.

Third-party providers should demonstrate appropriate security and data protection arrangements.

---

19. Data Subject Rights

Individuals have rights under UK data protection law, subject to applicable conditions and exemptions.

These may include the right to:

- Be informed about how their data is used.
- Access their personal data.
- Request correction of inaccurate information.
- Request deletion in certain circumstances.
- Request restriction of processing in certain circumstances.
- Object to certain processing.
- Request data portability in applicable circumstances.
- Challenge certain automated decision-making and profiling.

Requests will be handled in accordance with applicable legal requirements.

---

20. Subject Access Requests

An individual may request access to the personal information Anchoreach C.I.C. holds about them.

Requests should be passed promptly to the appropriate Director or person responsible for data protection.

The organisation will:

1. Record the request.
2. Verify the individual's identity where necessary.
3. Identify relevant information.

4. Review the information for third-party data and applicable exemptions.
5. Provide the information securely.
6. Keep a record of the response.

Anchoreach C.I.C. will normally respond within the applicable statutory timescale.

---

21. Requests to Correct Information

If an individual believes their information is inaccurate, they may request that it is corrected.

Anchoreach C.I.C. will review the information and make appropriate corrections where necessary.

Relevant records and systems should be updated where reasonably possible.

---

22. Requests for Deletion

Individuals may request deletion of their personal information in certain circumstances.

Deletion is not an absolute right.

Anchoreach C.I.C. may need to retain information where there is a legal, contractual, safeguarding or other legitimate requirement to do so.

Requests will be considered individually and responded to in accordance with applicable legislation.

---

23. Data Retention

Personal information will not be retained indefinitely.

Anchoreach C.I.C. will retain information for as long as it is reasonably necessary for the purpose for which it was collected, taking into account:

- Legal requirements.
- Funding requirements.
- Contractual requirements.
- Safeguarding considerations.
- Accounting requirements.

- Insurance requirements.
- Potential legal claims.
- Organisational needs.

When information is no longer required, it will be securely deleted, destroyed or anonymised where appropriate.

---

24. Data Breaches

A personal data breach may include:

- Loss of personal information.
- Theft of a device containing personal information.
- Sending information to the wrong person.
- Unauthorised access to a database.
- Accidental disclosure.
- Hacking or malware.
- Loss of paper records.
- Unauthorised alteration or deletion of information.

All suspected breaches must be reported immediately to a Director or the person responsible for data protection.

Staff and volunteers must not attempt to conceal a breach.

---

25. Data Breach Procedure

When a breach is identified:

Step 1 – Report

The person discovering the breach must report it immediately.

Step 2 – Contain

Reasonable steps should be taken to prevent further loss or disclosure.

For example:

- Recall an incorrectly sent email where possible.
- Change compromised passwords.
- Disconnect an affected device from a network where appropriate.

- Recover lost paperwork where possible.

Step 3 – Assess

Anchoreach C.I.C. will assess:

- What information was involved.
- How many individuals may be affected.
- The sensitivity of the information.
- What happened.
- The likely impact on individuals.
- What measures have already been taken.

Step 4 – Notify

Where legally required, Anchoreach C.I.C. will notify the **Information Commissioner's Office (ICO)** within the applicable statutory timescale.

Where a breach is likely to result in a high risk to affected individuals, those individuals will also be informed where required.

Step 5 – Record

All relevant breaches will be recorded, including breaches that do not require notification to the ICO.

Step 6 – Learn

The organisation will identify what can be done to prevent a similar breach occurring again.

---

26. Data Protection by Design

When introducing a new project, service, system or process involving personal information, Anchoreach C.I.C. will consider data protection from the beginning.

This may include:

- Minimising the information collected.
- Limiting access.
- Considering security risks.
- Providing privacy information.
- Checking third-party providers.
- Considering whether a Data Protection Impact Assessment (DPIA) is appropriate.

---

27. Data Protection Impact Assessments

A DPIA may be required where proposed processing is likely to result in a high risk to individuals.

Examples may include introducing new technology, large-scale processing of sensitive information or significant monitoring activities.

Where required, the organisation will complete an appropriate assessment before processing begins.

---

28. CCTV and Images

Where CCTV is used by Anchoreach C.I.C., it will be operated in accordance with data protection requirements and the organisation's CCTV procedures.

Appropriate signage will be displayed where required.

Access to CCTV footage will be restricted to authorised individuals.

Requests for CCTV footage will be handled in accordance with applicable data protection requirements.

---

29. Staff, Volunteer and Participant Records

Personal information relating to staff, volunteers and participants must only be accessed where necessary for legitimate organisational purposes.

Records may include:

- Contact details.
- Emergency contacts.
- Attendance.
- Training.
- Qualifications.
- Support requirements.
- Performance information.
- DBS-related information where applicable.
- Payment or expense information.
- Project monitoring information.

Sensitive information must receive appropriate additional protection.

30. Training and Responsibilities

All staff, directors and volunteers who handle personal information must understand their responsibilities.

Training and guidance may cover:

- UK GDPR principles.
- Confidentiality.
- Secure handling of information.
- Password security.
- Email security.
- Data breaches.
- Subject access requests.
- Photographs and social media.
- Safeguarding and information sharing.

---

31. Responsibilities

Board of Directors

The Board is responsible for ensuring that Anchoreach C.I.C. has appropriate data protection arrangements and resources.

Data Protection Lead

The organisation will appoint an appropriate person to oversee data protection arrangements.

Data Protection Lead: _____

Their responsibilities may include:

- Monitoring compliance.
- Maintaining data protection procedures.
- Supporting staff and volunteers.
- Coordinating data breach responses.
- Maintaining records.
- Supporting data subject requests.
- Reviewing policies and procedures.

- Advising the Board on data protection matters.

Staff and Volunteers

All staff and volunteers are responsible for:

- Following this policy.
- Protecting personal information.
- Maintaining confidentiality.
- Reporting suspected breaches immediately.
- Only accessing information required for their role.
- Completing relevant training.

---

32. Breaches of This Policy

Failure to follow this policy may result in action under relevant organisational procedures.

Serious or deliberate misuse of personal information may result in disciplinary action, removal from volunteering duties or termination of employment or contractual arrangements.

Where appropriate, serious incidents may be reported to external authorities.

---

33. Data Protection Checklist for Staff and Volunteers

Before handling personal information, staff and volunteers should ask:

- Do I need this information?
- Do I have a lawful reason to use it?
- Am I only using it for the purpose it was collected?
- Is the information accurate?
- Does anyone else need access?
- Am I storing it securely?
- Am I sharing only what is necessary?
- Could the information be anonymised?
- Do I need to keep it?
- Have I reported any suspected breach?

---

34. Data Protection Procedure – Quick Reference

Personal information received

↓

Identify why it is needed and the lawful basis

↓

Collect only necessary information

↓

Provide appropriate privacy information

↓

Store securely

↓

Limit access to authorised people

↓

Use and share only for legitimate purposes

↓

Respond appropriately to individual rights requests

↓

Report suspected breaches immediately

↓

Review and improve data protection arrangements

↓

Securely delete, destroy or anonymise information when no longer required

---

35. Monitoring and Review

Anchoreach C.I.C. will monitor its data protection arrangements and review this policy at least annually.

The policy will also be reviewed following:

- Significant changes in legislation.
- A serious data breach.
- Introduction of new technology or systems.
- Significant changes to services.
- Changes in organisational structure.
- Guidance issued by the ICO.

---

36. Approval

Organisation: Anchoreach C.I.C.
Policy: GDPR and Data Protection Policy and Procedures
Version: 1.0

Approved by: Board of Directors

Signature: P Marriner

Name: Paul Marriner

Position: Managing Director

Date: 17/08/2026

Review Date: 17/08/2027