Bright Steps CIC

Mentoring Today, Inspiring Tomorrow

# Data Protection & UK GDPR Policy and Procedures

**Document Control**

| | |
|---|---|
| **Document Title:** | **Data Protection & UK GDPR Policy and Procedures** |
| **Document Identifier** | **GC-01** |
| **Document Version:** | **Version 2.1** |
| **Author:** | **Elizabeth Spowage** |
| **Signature:** |  |
| **Date:** | **19/04/2026** |

| | |
|---|---|
| **Last Review Date** | **28/02/2026** |
| **Next Review Date** | **February 2027** |

Bright Steps CIC
Mentoring Today, Inspiring Tomorrow

# Table of Contents

## Contents

# 1. Policy Statement

Bright Steps Devon CIC ("Bright Steps") is committed to protecting the privacy, dignity and rights of the young people, families, staff, volunteers, trustees and partners we work with.

As an organisation supporting children and young people aged 8–25, including those with SEND and SEMH needs, we recognise that we process sensitive and special category data. We take our responsibilities under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 seriously.

We are registered with the Information Commissioner's Office (ICO) and comply with all applicable data protection legislation.

# 2. Purpose

This policy sets out:

- How Bright Steps complies with UK GDPR principles
- How personal and special category data is processed
- Roles and responsibilities within the organisation
- Security, retention and breach procedures
- Individual rights and how they are upheld

This is an internal governance policy and should be read alongside:

- Safeguarding Policy
- Confidentiality Policy
- IT & Acceptable Use Policy
- Records Retention Schedule
- Privacy Notice (external document)

# 3. Scope

This policy applies to all personal data processed by Bright Steps, whether held:

- Electronically (Microsoft 365 / SharePoint / email systems)
- In paper format
- On mobile devices
- Within third-party systems (e.g., payroll, accounting, DBS)

It applies to data relating to:

- Young people
- Parents and carers
- Staff
- Volunteers and associates
- Trustees
- Referrers and partners

- Contractors and suppliers

# 4. Definitions

**Personal Data** – Any information relating to an identified or identifiable person.
**Special Category Data** – Sensitive data including health, SEND status, safeguarding information, ethnicity, or other protected characteristics.
**Processing** – Any operation performed on data (collection, storage, sharing, deletion).
**Data Controller** – Bright Steps Devon CIC.
**Data Processor** – A third party processing data on our behalf.

# 5. Data Protection Principles

Bright Steps Devon CIC will comply with the UK GDPR and Data Protection Act 2018 by applying the seven data protection principles to all personal data processing activities. These principles underpin how we collect, use, store, share and dispose of personal data, and they apply to both electronic and paper records.

## 5.1 Lawfulness, Fairness and Transparency

Bright Steps will:

- Process personal data only where a valid lawful basis applies (and where relevant, a special category condition).
- Provide clear information to individuals about how their data is used through an appropriate Privacy Notice and service documentation.
- Ensure processing is fair and does not have unjustified adverse impacts on individuals.

## 5.2 Purpose Limitation

Bright Steps will:

- Collect personal data for specified and legitimate purposes linked to service delivery, safeguarding, legal compliance and organisational management.
- Not use personal data for unrelated purposes without a lawful basis (and where required, further information to individuals).
- Review any proposed new use of data to ensure compatibility with the original purpose and document decisions where appropriate.

## 5.3 Data Minimisation

Bright Steps will:

- Collect and record only the minimum amount of personal data required to deliver services safely and effectively.
- Avoid excessive, irrelevant or speculative recording, including within session notes.
- Use anonymised or pseudonymised data for monitoring, reporting and evaluation wherever possible.

## 5.4 Accuracy

Bright Steps will:

- Take reasonable steps to ensure personal data is accurate, complete and kept up to date.
- Update records promptly when new information is received or when inaccuracies are identified.
- Provide mechanisms for individuals to request correction and ensure corrections are recorded appropriately.

## 5.5 Storage Limitation

Bright Steps will:

- Retain personal data only for as long as necessary for the purpose it was collected, in line with our Records Retention Schedule.
- Review retention periods periodically and securely dispose of data when it is no longer required.
- Retain safeguarding and child protection information in accordance with statutory guidance and organisational safeguarding procedures.

## 5.6 Integrity and Confidentiality

Bright Steps will:

- Protect personal data against unauthorised access, unlawful processing, loss, destruction or damage.
- Apply appropriate technical and organisational measures including access controls, secure storage, encrypted devices where applicable, and secure disposal.
- Restrict access to personal and special category data on a strict “need to know” basis, including role-based access permissions within SharePoint and associated systems.

## 5.7 Accountability

Bright Steps will:

- Maintain appropriate records to demonstrate compliance, including Records of Processing Activities (ROPA) where required, a breach log, and data sharing documentation.
- Ensure data protection responsibilities are reflected in induction, training and ongoing supervision.
- Monitor compliance through periodic review, learning from incidents, and updating policies and procedures where needed.

# 6. Lawful Bases for Processing

Bright Steps will identify and document a lawful basis (and where relevant, a special category condition) before processing personal data. The lawful basis used will depend on the purpose for processing and the relationship with the individual.

Bright Steps may rely on one or more of the following lawful bases:

## 6.1 Contract

We may process personal data where it is necessary to:

- Deliver mentoring, enabling and support services agreed with a young person, parent/carer, commissioner or referrer.
- Administer referrals, sessions, service plans, communications and delivery arrangements.
- Manage associated service documentation and agreed outcomes.

## 6.2 Legal Obligation

We may process personal data where necessary to comply with legal and regulatory duties, including:

- Safeguarding and child protection responsibilities.
- Employment law obligations (including right to work checks, payroll and HR records).
- Tax and accounting requirements.
- DBS checking and safer recruitment processes.
- Cooperation with statutory bodies where required by law (e.g., court orders).

## 6.3 Legitimate Interests

We may process personal data where it is necessary for Bright Steps' legitimate interests and those interests are not overridden by the individual's rights and freedoms. This may include:

- Operating services safely and effectively.
- Quality assurance, supervision and case management.
- Service evaluation, performance monitoring and reporting (using anonymised data wherever possible).
- Maintaining organisational security, IT access control and audit trails.
- Preventing fraud, misuse of services or safeguarding-related risk.

Where we rely on legitimate interests, we will consider and balance the impact on the individual and document this where appropriate.

## 6.4 Consent

We will use consent only where it is appropriate and genuinely optional. Consent may be used for:

- Photographs, video or media/publicity activity.
- Non-essential communications (e.g., newsletters where applicable).
- Optional activities or data uses that are not required for core service delivery.

Where consent is used, Bright Steps will ensure it is:

- Freely given, specific, informed and unambiguous.
- Recorded clearly.
- Capable of being withdrawn at any time (and withdrawal will be respected promptly).

**Important:** Bright Steps will not normally rely on consent as the lawful basis for core safeguarding-related processing or essential service delivery where another lawful basis is more appropriate.

# 7. Special Category Data

Bright Steps works with children, young people and families where support needs and risk factors may require the processing of special category personal data (and in some cases, criminal offence data). We recognise that this information requires a higher standard of protection.

## 7.1 Types of Special Category Data We May Process

Depending on the nature of the support provided, Bright Steps may process:

- Health and wellbeing information (including mental health and emotional wellbeing needs)
- SEND information, including disability-related information and EHCP-related details
- Safeguarding and child protection information, including disclosures and concerns
- Social care involvement and information provided by partner agencies
- Risk assessments, safety plans and incident records
- Diversity and equality information where required for monitoring or support planning (minimised wherever possible)

## 7.2 Conditions for Processing Special Category Data (UK GDPR Article 9)

Where special category data is processed, Bright Steps will ensure that:

1. a lawful basis under Article 6 is identified (see Section 6), and
2. an additional condition under Article 9 applies.

Bright Steps may rely on one or more of the following Article 9 conditions, as appropriate:

- **Article 9(2)(g) – Substantial public interest,** including safeguarding of children and individuals at risk (with appropriate policy safeguards).
- **Article 9(2)(h) – Health or social care purposes**, where information supports safe and appropriate delivery of wellbeing, support or care-related activity.

- **Article 9(2)(b) – Employment, social security and social protection law**, where relevant to staff/volunteer management and legal duties.
- **Article 9(2)(a) – Explicit consent**, only where the processing is genuinely optional and consent can be freely given and withdrawn without detriment (e.g., particular optional activities or additional support elements).

**Important:** Bright Steps will not normally rely on explicit consent for safeguarding-related processing where another lawful basis and condition is more appropriate.

### 7.3 Criminal Offence Data

Where Bright Steps processes information relating to criminal convictions or offences (for example within safeguarding records or safer recruitment/DBS processes), this will be handled in accordance with the Data Protection Act 2018, with access restricted to those who require it for safeguarding or employment purposes.

### 7.4 Additional Safeguards

Bright Steps applies enhanced controls for special category and safeguarding-related information, including:

- Role-based access controls and "need to know" permissions (including within SharePoint)
- Secure storage arrangements for paper records (locked storage)
- Secure organisational IT accounts, strong passwords and multi-factor authentication where enabled
- Clear confidentiality expectations, including confidentiality clauses/agreements for staff, volunteers and associates
- Controlled information sharing arrangements linked to safeguarding procedures, with decisions recorded
- Minimised recording in session notes (relevant, factual, proportionate)
- Secure disposal procedures (secure deletion/shredding)

## 8. Roles and Responsibilities

Bright Steps ensures that data protection is managed as a core governance responsibility. All directors, staff, volunteers and associates must understand their role in protecting personal data and supporting compliance with UK GDPR and the Data Protection Act 2018.

### 8.1 Board of Directors

The Board of Directors will:

- Hold ultimate accountability for data protection compliance across Bright Steps.
- Ensure appropriate policies, procedures and resources are in place to meet legal requirements.
- Receive assurance that data protection risks are identified, managed and reviewed, including learning from any incidents or breaches.

- Ensure data protection responsibilities are embedded within organisational governance and risk management.

## 8.2 Data Protection Lead (Director)

The Director acts as Bright Steps' Data Protection Lead and is responsible for:

- Overseeing organisational compliance with UK GDPR and the Data Protection Act 2018.
- Ensuring an appropriate Privacy Notice is maintained and available to individuals.
- Maintaining the ICO registration and ensuring accuracy of registration details.
- Managing and responding to Subject Access Requests (SARs) and other data rights requests within statutory timeframes.
- Managing personal data breaches, including assessment, logging, notifications (ICO/individuals where required), and corrective actions.
- Ensuring staff/volunteers/associates receive appropriate induction, training and guidance.
- Approving and overseeing data sharing arrangements and ensuring appropriate agreements are in place with third parties where required.
- Ensuring retention and secure disposal arrangements are implemented in line with the Records Retention Schedule.
- Reviewing this policy at least annually (or earlier if there are significant changes, incidents, or regulatory updates).

## 8.3 Staff, Volunteers and Associates

All staff, volunteers and associates must:

- Process personal data only as necessary for their role and in line with Bright Steps policies and instructions.
- Maintain confidentiality and apply a strict "need to know" approach to access and sharing.
- Keep information secure in all formats (digital, paper and verbal), including safe handling of devices and records.
- Use only approved systems for storing and sharing information (e.g., Bright Steps SharePoint) and avoid personal email accounts or unapproved storage.
- Ensure records, session notes and communications are relevant, factual and proportionate, and do not include unnecessary personal detail.
- Report suspected or actual data breaches immediately to the Director, without delay.
- Complete required data protection and confidentiality training, including refresher training where required.

## 8.4 Third-Party Processors, Contractors and Delivery Partners

Where Bright Steps uses third parties to support delivery (including associates, subcontractors, professional services, IT providers, HR/payroll/accounting support, or

partner agencies), Bright Steps will ensure that personal data is protected and processed lawfully.

Bright Steps will:

- Confirm whether the third party is acting as a Data Processor, Joint Controller or Independent Controller, and document the arrangement appropriately.
- Put in place appropriate written terms, including a Data Processing Agreement (DPA) where the third party is processing personal data on Bright Steps' behalf.
- Ensure third parties only process data on documented instructions from Bright Steps (where acting as a processor).
- Ensure third parties apply appropriate security measures and confidentiality obligations, including secure storage, access controls and incident reporting.
- Ensure third parties report any suspected or actual data breach to Bright Steps immediately, and cooperate with investigation and notifications.
- Limit data sharing to what is necessary and proportionate for the agreed purpose ("minimum necessary" approach).
- Require safe return or secure deletion of personal data when the service ends, in line with retention requirements and contractual terms.

Non-compliance with this policy may result in formal action, including disciplinary procedures and/or termination of engagement (as applicable), and may be reported to relevant authorities where required.

# 9. Data Security

Bright Steps will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access. Security controls are applied proportionately, recognising that Bright Steps processes special category and safeguarding-related information.

## 9.1 Secure Systems and Storage

Bright Steps will:

- Use a Microsoft 365 environment for organisational email, document storage and collaboration.
- Store operational records in SharePoint (and approved organisational systems only), using role-based access permissions.
- Restrict access to personal and special category data on a strict "need to know" basis.
- Maintain secure storage for any paper records, including locked cabinets and controlled access areas.

## 9.2 Account Security and Access Controls

Bright Steps will:

- Ensure each staff member/associate uses their own named organisational account (no shared logins).
- Require strong passwords and apply multi-factor authentication (MFA) where enabled/available.
- Remove or amend access promptly when roles change or engagement ends.
- Apply appropriate controls for remote working, including secure access and appropriate device use.

### 9.3 Device and Mobile Working Security

Bright Steps will:

- Require that laptops, tablets and phones used for Bright Steps work are protected with passwords/PINs and automatic locking.
- Use encryption where applicable and available, particularly for portable devices.
- Prohibit storing sensitive information locally where it can reasonably be stored securely within SharePoint.
- Require immediate reporting of lost/stolen devices that may contain, or provide access to, personal data.

### 9.4 Email, Messaging and Information Transfer

Bright Steps will:

- Use organisational email accounts for business communications and avoid forwarding personal data to personal email addresses.
- Share documents using secure links and controlled access rather than unprotected attachments where possible.
- Verify recipient details before sending personal data and limit content to what is necessary.

### 9.5 Physical Security and Clear Desk Practice

Bright Steps will:

- Maintain a clear desk approach where practicable.
- Store printed records securely when not in use.
- Ensure confidential waste is disposed of securely and not placed in general waste.

### 9.6 Secure Disposal

Bright Steps will:

- Dispose of paper records via secure shredding.
- Dispose of electronic records via secure deletion in line with retention requirements and approved processes.
- Ensure third parties return or securely delete information at the end of their service arrangement where applicable.

### 9.7 Security Incidents and Reporting

A security incident is any event that could compromise the confidentiality, integrity or availability of personal data, whether or not a confirmed breach has occurred. This includes (but is not limited to):

- Misdirected emails or messages containing personal data
- Lost or stolen devices, paperwork or notebooks
- Unauthorised access (or suspected access) to files or accounts
- Accidental deletion or alteration of records
- Phishing attempts, malware alerts, or suspicious links
- Sharing information via unapproved platforms or accounts
- Any "near miss" where harm was avoided but the risk was present

All personnel must report any suspected or actual security incident immediately to the Director/Data Protection Lead. Staff should report concerns even if they are unsure whether the incident meets the threshold for a personal data breach.

The Director/Data Protection Lead will:

- Take immediate steps to contain risk (e.g. revoke access, recover documents, isolate devices)
- Assess whether the incident constitutes a personal data breach
- Ensure the incident is recorded in the Security Incident/Breach Log
- Implement corrective actions, learning and improvements to reduce recurrence

## 10. Data Sharing

Bright Steps shares personal data only where it is lawful, necessary and proportionate. Information sharing decisions will be made in a way that supports safe service delivery and safeguarding, while respecting individual rights and confidentiality.

### 10.1 When Bright Steps May Share Personal Data

Bright Steps may share personal data where one or more of the following applies:

- Consent has been provided and can be freely given and withdrawn (where consent is the appropriate basis).
- Safeguarding concerns require information to be shared to protect a child or young person or others from harm, in line with safeguarding duties and relevant guidance.
- Sharing is required by law (for example, where compelled by a court order or statutory requirement).
- Sharing is necessary for service delivery, case coordination, or commissioning requirements (for example with schools, Local Authorities, health or social care professionals), where a lawful basis applies and the sharing is proportionate.

Bright Steps will never sell personal data and will not share personal data for marketing by third parties.

## 10.2 Safeguarding and Confidentiality

Where safeguarding concerns arise, Bright Steps may share relevant information without consent if doing so is necessary to protect a child or young person or others. In such cases:

- The safety and welfare of the child/young person is prioritised.
- Only the minimum necessary information is shared.
- The rationale for sharing (including why consent was not sought or could not be obtained) is recorded.

## 10.3 Minimum Necessary and Secure Transfer

When sharing information, Bright Steps will:

- Share only what is relevant and necessary for the purpose.
- Verify the identity and role of the recipient before disclosure.
- Use secure methods for transfer (e.g., controlled-access links, secure email arrangements where available).
- Apply confidentiality markings where appropriate and restrict onward sharing.

## 10.4 Recording and Authorisation

Bright Steps will record:

- What information was shared and with whom
- The purpose and lawful basis for sharing
- Whether consent was obtained, and if not, the reason
- Any conditions placed on use or onward sharing

Information sharing must be authorised in line with internal arrangements. As a minimum:

- Routine operational sharing for delivery may be undertaken by staff/associates within their role and in line with this policy.
- Non-routine, sensitive or safeguarding-related disclosures must be escalated to, or agreed with, the Director/Data Protection Lead.

## 10.5 Third Parties: Processors, Controllers and Agreements

Where Bright Steps uses third parties to process data on our behalf (e.g., IT, payroll, accounting platforms, contracted delivery associates where acting under instruction), Bright Steps will ensure:

- The relationship is clearly defined as Processor, Joint Controller, or Independent Controller.
- A Data Processing Agreement (DPA) is in place where required, setting out confidentiality, security standards, breach reporting, and deletion/return requirements.
- Data is shared only to the extent necessary to fulfil the agreed service.

## 10.6 Common Information Sharing Scenarios

Bright Steps recognises that information sharing decisions in children and young people's services can be complex. The following scenarios set out expectations for common situations. In all cases, Bright Steps will share only what is necessary, use secure methods, and record the decision-making.

### 10.6.1 Sharing with Schools, Colleges and Alternative Provision

Bright Steps may share relevant information with education settings where it supports:

- Safe and effective delivery of teaching/mentoring/enabling support
- Attendance, wellbeing, behaviour and support planning
- Agreed outcomes and review processes

Sharing will be limited to what is necessary for the agreed purpose and will follow the lawful basis identified for the service.

### 10.6.2 Sharing with Local Authorities and Commissioning Bodies

Where services are commissioned or funded, Bright Steps may share:

- Progress updates and outcome reporting
- Attendance/engagement information
- Safeguarding-relevant concerns (where required)

Where possible, Bright Steps will use anonymised or aggregated data for reporting. Personal data will only be shared where it is necessary and lawful.

### 10.6.3 Sharing with Health and Social Care Professionals

Bright Steps may share information with health or social care professionals to:

- Support joined-up working and risk management
- Coordinate support plans and wellbeing needs
- Escalate safeguarding concerns

Information will be shared proportionately and with appropriate safeguards.

### 10.6.4 Safeguarding: Sharing Without Consent

If Bright Steps believes a child or young person is at risk of harm, information may be shared without consent where necessary. Where appropriate and safe, Bright Steps will be transparent with the child/young person and/or parent/carer about what has been shared and why.

### 10.6.5 Requests from Parents/Carers

Bright Steps will handle parent/carer requests carefully and lawfully. We will consider:

- The age and understanding of the young person
- Whether the young person has capacity to make decisions about their data
- Any safeguarding concerns or risks arising from disclosure
- Whether the requesting adult has parental responsibility (where relevant)

Bright Steps will not disclose information where doing so would put the young person or others at risk, breach confidentiality without a lawful basis, or conflict with safeguarding obligations.

#### 10.6.6 Separated Parents and Parental Responsibility

Where parents/carers are separated or there is disagreement, Bright Steps will:

- Seek clarity on parental responsibility where relevant
- Avoid sharing information in a way that escalates conflict or creates risk
- Consider legal restrictions (e.g., court orders) where known
- Escalate to the Director/Data Protection Lead for non-routine or sensitive disclosures

#### 10.6.7 Young People Aged 16–25

For young people aged 16 and over, Bright Steps will generally treat the young person as the primary decision-maker about their information, unless:

- There is a safeguarding concern requiring sharing
- The young person lacks capacity to understand the decision
- Another lawful requirement applies

Where appropriate, Bright Steps will encourage supportive involvement of parents/carers, but will respect the young person's rights and confidentiality.

#### 10.6.8 Media, Publicity and Case Studies

Bright Steps will not use identifiable information (including photographs/video) for publicity or case studies unless appropriate consent has been obtained and recorded. Consent can be withdrawn, and Bright Steps will act promptly to stop further use.

# 11. Data Retention

Bright Steps will retain personal data only for as long as it is necessary for the purpose for which it was collected, and in accordance with the UK GDPR principle of storage limitation. Retention periods are set out in the Bright Steps Records Retention Schedule, which is maintained and reviewed by the Director/Data Protection Lead.

- Retention decisions will take account of:
- Safeguarding responsibilities and statutory guidance
- Legal and regulatory duties (including employment and financial recordkeeping)
- Commissioning/funder requirements (where applicable and lawful)
- The need to evidence decisions and service delivery where appropriate

## 11.1 General Retention Periods (Guidance)

As a general guide, Bright Steps will retain:

- **Young person service records** (including referral documentation, support plans, key communications, and session records):

normally 6 years after the service ends, and longer where safeguarding, risk, complaint, dispute, or legal requirements indicate.

- **Safeguarding/child protection records:**
  retained in line with statutory guidance and organisational safeguarding procedures. Where safeguarding information is held, it will be kept securely and separately/appropriately flagged within the record structure to support controlled access.
- **Staff, volunteer and associate records:**
  retained in line with employment law, safer recruitment requirements, and organisational governance needs (including DBS and training records, where applicable).
- **Financial records** (including invoices, payroll records, and associated accounting documentation):
  retained for a minimum of 6 years in line with statutory accounting and tax requirements.

### 11.2 Review, Archiving and Secure Disposal

Bright Steps will:

- Review records periodically to confirm continued need and appropriate retention category.
- Archive records securely where active use has ended but retention is still required.
- Securely dispose of personal data once it is no longer required, using:
  - Confidential shredding for paper records
  - Secure deletion for electronic records, including removal from any recycle/retention areas where applicable
- Ensure any third-party processors securely delete or return information at contract end in line with agreed terms.

### 11.3 Holds for Complaints, Incidents or Legal Matters

Where there is an ongoing safeguarding concern, complaint, incident investigation, insurance matter, dispute, or legal process, Bright Steps may place a retention hold on relevant records and retain them beyond the standard period until the matter is fully concluded and it is lawful to dispose of the information.

## 12. Subject Access Requests (SARs) and Individual Rights Requests

Bright Steps recognises and upholds the rights of individuals under UK GDPR in relation to their personal data. Requests may be received from young people, parents/carers, staff, volunteers, trustees, or other individuals whose data we hold.

## 12.1 Rights Under UK GDPR

Individuals may have the right to:

- **Access** their personal data (Subject Access Request)
- **Rectification** – request correction of inaccurate or incomplete data
- **Erasure** – request deletion of data (where lawful and applicable)
- **Restriction** – request restriction of processing in certain circumstances
- **Object** – object to processing in certain circumstances (including where legitimate interests applies)
- **Data portability** – receive certain data in a portable format (where applicable)

These rights are not absolute and may be limited by law (for example, where disclosure would identify another person, prejudice safeguarding, or conflict with legal obligations).

## 12.2 How to Make a Request

Requests should be made in writing (email or letter) to the Director/Data Protection Lead. Where requests are made verbally, Bright Steps will support the individual to put the request in writing and will record the date received.

## 12.3 Identity and Authority Checks

Before releasing information, Bright Steps may require:

- Proof of identity, and/or
- Evidence of authority to act on behalf of another person (e.g., parental responsibility, legal authority, power of attorney, or written consent)

For requests involving a child or young person, Bright Steps will consider:

- The young person's age, understanding and capacity to make decisions about their data
- Safeguarding risk and confidentiality considerations
- Whether the request is being made by a person with parental responsibility (where relevant)

Where there is uncertainty or sensitivity, the request will be escalated to the Director/Data Protection Lead.

## 12.4 Timescales and Extensions

Bright Steps will respond within one calendar month of:

- receiving the request, and
- completing any necessary identity verification.

If a request is complex or numerous, Bright Steps may extend the response time by up to two further months. Where this applies, Bright Steps will inform the requester within one month and explain the reason for the extension.

### 12.5 What Bright Steps Will Provide

Bright Steps will provide:

- Confirmation of whether personal data is being processed
- A copy of relevant personal data (subject to lawful exemptions)
- Supporting information required by UK GDPR (e.g., purposes of processing, recipients, retention, rights)

Bright Steps will take reasonable steps to:

- Redact third-party personal data where disclosure would identify another person
- Withhold information where a lawful exemption applies (e.g., safeguarding-related risk, legal privilege)

### 12.6 Fees and Refusal

Bright Steps will not normally charge a fee, however a reasonable fee may be charged, or a request refused, where it is manifestly unfounded or excessive, in line with UK GDPR. Any refusal will be explained clearly, with information on the right to complain to the ICO.

### 12.7 Recording and Governance

Bright Steps will:

- Maintain a log of SARs and rights requests, including dates, actions taken and outcomes
- Ensure requests are managed confidentially and securely
- Use learning from requests to improve recordkeeping and transparency

## 13. Personal Data Breaches

A personal data breach is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This may include breaches involving special category or safeguarding-related information.

### 13.1 Immediate Reporting Requirement

All staff, volunteers and associates must report any suspected or actual personal data breach immediately to the Director/Data Protection Lead. Concerns must be reported even where the individual is unsure whether the incident meets the definition of a breach.

Examples include (but are not limited to):

- Email sent to the wrong recipient containing personal data
- Loss/theft of a device, paperwork or notebook
- Unauthorised access to files, accounts or folders
- Sharing information via an unapproved channel
- Accidental deletion or corruption of personal data where it cannot be recovered

## 13.2 Containment and Initial Actions

On becoming aware of a suspected breach, Bright Steps will take prompt steps to contain and reduce risk, which may include:

- Recalling or securing mis-sent information where possible
- Resetting passwords and revoking access
- Recovering documents/devices
- Isolating devices/accounts where compromise is suspected
- Preserving evidence for investigation

## 13.3 Assessment and Decision-Making

The Director/Data Protection Lead will assess:

- The nature and volume of data involved
- Whether special category/safeguarding data is included
- The number of individuals affected
- Likely consequences and risk of harm (including distress, discrimination, identity theft, reputational harm, or safeguarding risk)
- Whether the data was protected (e.g., encryption, access controls)

## 13.4 Recording and Breach Log

All suspected and confirmed breaches will be recorded in the Breach Log, including:

- Date/time of incident and discovery
- What happened and what data was involved
- Who was affected
- Containment actions taken
- Risk assessment and outcome
- Notifications made (ICO/individuals/partners)
- Corrective and preventive actions

## 13.5 ICO Notification (72 hours)

Where a breach is likely to result in a risk to the rights and freedoms of individuals, Bright Steps will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where notification is not made, Bright Steps will document the decision and rationale.

## 13.6 Notification to Individuals

Where a breach is likely to result in a high risk to individuals, Bright Steps will notify affected individuals without undue delay, providing:

- A clear description of what happened
- What information was involved
- Steps Bright Steps has taken to address it

- Actions individuals can take to protect themselves
- How to contact Bright Steps for support

### 13.7 Learning and Improvement

Following any breach (or significant near miss), Bright Steps will implement corrective actions which may include:

- Updating procedures and permissions
- Additional staff training and supervision
- Technical/security improvements
- Updates to risk assessments and DPIAs where relevant

### 13.8 Safeguarding-Linked Breaches

Where a personal data breach involves safeguarding information or could increase the risk of harm to a child, young person, or others, Bright Steps will treat the incident as a heightened risk matter.

In addition to the actions set out above, the Director/Data Protection Lead will:

- Consider whether immediate safeguarding actions are required to protect the child/young person (including escalation under the Safeguarding Policy).
- Consider whether information must be shared with relevant safeguarding partners (e.g., children's social care, police, DSL at the education setting), where lawful and necessary.
- Ensure that safeguarding decision-making and any information sharing is clearly recorded, including the rationale and actions taken.
- Notify the Board of Directors where the breach is serious, involves significant safeguarding risk, or is likely to attract regulatory attention.

Where appropriate, Bright Steps will align any breach response with safeguarding reporting routes and ensure that data protection actions do not delay urgent protective steps.

## 14. Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a structured process used to identify and minimise data protection risks. Bright Steps will complete a DPIA where processing is likely to result in a high risk to individuals' rights and freedoms, particularly where children and young people or special category data are involved.

### 14.1 When a DPIA Will Be Completed

Bright Steps will undertake a DPIA where processing includes, or is likely to include:

- Processing that is high risk due to the nature, scope, context or purposes of the activity

- Processing involving children, young people or vulnerable individuals, especially where risk and welfare information is recorded
- Large-scale processing of special category data (relative to the organisation's size and service model)
- Introducing new systems, platforms or technologies (e.g., new apps, case management tools, new storage/sharing approaches)
- Significant changes to how data is collected, shared, stored or accessed (including new partners or delivery models)
- Any activity that involves systematic monitoring, profiling, or extensive decision-making using personal data

### 14.2 Responsibility and Approval

The Director/Data Protection Lead is responsible for ensuring DPIAs are completed where required and that risks and controls are documented before processing begins. Where delivery partners or contractors are involved, they may be required to contribute to the DPIA process.

### 14.3 What a DPIA Will Cover

A DPIA will document:

- The purpose of the processing and intended outcomes
- The data involved (including special category data) and who it relates to
- The lawful basis and special category condition(s) relied upon
- Data flows, storage locations, access permissions and sharing arrangements
- Risks to individuals (including safeguarding and confidentiality risks)
- Measures to reduce risk (security controls, minimisation, retention, access controls, training)
- The final risk rating and sign-off decision

### 14.4 Managing Residual High Risk

Where a DPIA identifies that high risk remains despite mitigation, Bright Steps will:

- Review whether the processing can be redesigned to reduce risk further, and/or
- Seek appropriate advice and, where required, consult the ICO before proceeding.

DPIAs will be reviewed and updated where there are material changes to the processing activity or new risks emerge.

## 15. Training and Awareness

Bright Steps recognises that effective data protection depends on staff understanding and day-to-day practice. All staff, volunteers, trustees and associates will receive appropriate training and guidance to ensure personal data is handled lawfully, securely and consistently.

### 15.1 Induction

All new starters will complete induction covering, as a minimum:

- UK GDPR/data protection basics and confidentiality expectations
- Secure working practices (including SharePoint use, email hygiene, and device security)
- Recognising and reporting security incidents and data breaches
- Safeguarding-linked information sharing and recording standards

### 15.2 Ongoing Awareness and Reinforcement

Bright Steps will reinforce good practice through:

- Supervision, line management and case discussion (including recordkeeping standards)
- Periodic reminders on key risks (e.g., phishing, mis-sent emails, secure storage)
- Updates where systems, processes, or guidance change

### 15.3 Refresher Training

Refresher training will be provided:

- At intervals determined by the organisation (as a minimum, periodically and when required), and
- Following any significant incident, near miss, or identified training need.

### 15.4 Training Records

Bright Steps will maintain records of completed training for staff, volunteers and associates, and will take action where training is overdue or where additional support is required.

## 16. Monitoring and Review

Bright Steps will monitor compliance with this policy and review its effectiveness to ensure ongoing alignment with UK GDPR, the Data Protection Act 2018, and recognised good practice for organisations supporting children and young people.

### 16.1 Policy Review

This policy will be reviewed at least annually by the Director/Data Protection Lead and approved in accordance with Bright Steps governance arrangements. It will also be reviewed sooner where:

- There are changes to relevant legislation or case law
- ICO guidance or regulatory expectations change
- There are significant operational or organisational changes (e.g., new services, systems, delivery models, or partners)
- A serious data breach occurs, or there are repeated incidents/near misses

- An audit, complaint, inspection or funder requirement identifies a need for amendment

### 16.2 Compliance Monitoring

To provide assurance that arrangements remain effective, Bright Steps may undertake proportionate monitoring activities, which may include:

- Periodic checks of access permissions and secure storage arrangements
- Spot checks of recordkeeping quality (e.g., session notes being factual, proportionate and relevant)
- Review of the incident/breach log and actions taken
- Review of training completion and emerging training needs
- Review of data sharing arrangements and agreements where applicable

Learning from monitoring and incidents will be used to improve processes, strengthen controls and update training and guidance.

## 17. Related Documents

This policy should be read alongside the following Bright Steps policies, procedures and templates (as applicable):

- Safeguarding Policy (including information sharing and recording expectations)
- Confidentiality Policy / Code of Conduct
- IT & Acceptable Use Policy (including remote working and device security requirements)
- Records Retention Schedule
- External Privacy Notice (young people, parents/carers, referrers, website users as relevant)
- Data Breach / Security Incident Procedure and Log Template
- Subject Access Request (SAR) Procedure and Request Form
- Data Protection Impact Assessment (DPIA) Template

## 18. Appendices

The following appendices support the implementation of this policy and form part of the Bright Steps Data Protection & UK GDPR framework:

**Appendix A** – Data Sharing Decision Record Template
**Appendix B** – Subject Access Request (SAR) Request Form
**Appendix C** – Security Incident / Personal Data Breach Report Form
**Appendix D** – Data Protection Impact Assessment (DPIA) Template
**Appendix E** – Records Retention Schedule

# 19. Document Control and Update Record

## Document Information

| DOCUMENT TITLE | |
|---|---|
| **POLICY AREA** | GC-01 Data Protection & UK GDPR Policy and Procedures |
| **DOCUMENT OWNER** | Elizabeth Spowage |
| **APPROVED BY** | Board of Directors |
| **ORIGINAL APPROVAL DATE** | 11/09/25 |
| **REVIEW FREQUENCY** | Annual (or sooner if required) |
| **NEXT REVIEW DUE** | February 2027 |

## 2. Version Control Record

| VERSION | DATE | SECTION(S) UPDATED | SUMMARY OF CHANGES | APPROVED BY |
|---|---|---|---|---|
| **1.0** | 11/09/25 | Initial Document | Initial issue | Liz Spowage - Director |
| **2.0** | 28/02/26 | All Sections | Full Rewrite | Liz Spowage - Director |
| **2.1** | 19/04/26 | All Pages | Ver 2.0 issue date & Contact Details | Liz Spowage - Director |

## 3. Review History (Even if No Changes Made)

| REVIEW DATE | REVIEWER | OUTCOME | NOTES |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |