# Data Protection Policy

## 2026

## Contents

## Policy Statement

Integrating's Data Protection Policy has been produced to ensure compliance with the Data Protection Act 2018 (DPA), GDPR and associated legislation, and it incorporates guidance from the Information Commissioner's Office (ICO). The DPA gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

Personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e., as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored, or otherwise processed by the charity, or by a third party on its behalf.

This policy is designed to protect individuals from any damage or distress that might result from the process and transmission of their personal details. Compliance with this regulation is a legal requirement and we seek to meet all its responsibilities.

Special category data is personal data consisting of information relating to:

• racial or ethnic origin
• political opinions, religious beliefs, or other beliefs of a similar nature
• membership of a trade union
• physical or mental health or condition
• sexual orientation
• biometric /genetic data

## Policy Aims

This Policy applies to all employees working for, or on behalf of, the charity, third parties and others who may process personal information on behalf of Integrating. The Policy also covers any staff or volunteers and charity members who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the charity to ensure the data is processed in accordance with the DPA 2018 and that they are advised about their responsibilities.

- We will ensure that the requirements of the GDPR Regulations are in all respects observed.
- We will comply with the GDPR Principles
- We will ensure that employees are aware of our Policy and its requirements.
- Integrating will ensure that any external bodies which provides, receives or processes personal data from or on behalf of Integrating comply with the requirements of the GDPR Regulations.

Signed  Date **01.12.25**

Review Date **01.11.26**

## Procedures

### Roles and Responsibilities for Employees

- All employees have the responsibility to ensure that they comply with the principles and requirements of the Act.
- All employees will only process personal data to the extent to which they have been actively authorised by Integrating.
- All employees are responsible for complying with any security procedures implemented by Integrating.

### Principles

The eight Data Protection Principles are contained in Schedule 1 to the Act, the following being a summary.

The principles require that personal data shall be:

I. processed fairly and lawfully
II. obtained for specified and lawful purposes
III. adequate, relevant and not excessive
IV. accurate and up to date
V. not kept any longer than necessary
VI. processed in accordance with the 'data subject's' (the individual's) rights
VII. securely kept
VIII. not transferred to any other country without adequate protection being in place

### Implementation

- The responsibility for ensuring employment practices comply with the Data Protection Act lies with the Business Manager.
- The responsibility for processing employee records as regards registration under the Data Protection Act lies with the Business Manager.
- The responsibility for maintaining confidentiality as regards sensitive personal data as defined by the Act lies with Integrating including all its Trustees and employees.
- An audit of personal data and systems operated will be carried out at regular intervals to ensure compliance with the Act.

### Processing Data

Integrating has a Data Protection Officer to handle day-to-day issues which arise, and to provide members of the charity with guidance on Data Protection issues to ensure they are aware of their obligations.

All new members of staff will be required to complete a mandatory information governance module as part of their induction and existing staff will be requested to undertake refresher training on a regular basis.

Employees of Integrating are expected to:

- familiarise themselves and comply with the eight data protection principles
- ensure any possession of personal data is accurate and up to date
- ensure their own personal information is accurate and up to date
- keep personal data for no longer than is necessary
- ensure that any personal data they process is secure and in compliance with Integrating's information related policies and strategies
- acknowledge data subjects' rights (e.g., right of access to all their personal data held by the Academy) under the DPA 2018 and comply with access to records.
- ensure personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern Integrating
- obtain consent with collecting, sharing, or disclosing personal data
- contact the Business Manager with any concerns or doubt relating to data protection to avoid any infringements of the DPA 2018.

**Obtaining, Disclosing and Sharing**

Only personal data that is necessary for a specific charity related business reason should be obtained.

Parents/carers are informed about how their children's data will be processed when they agree to the Data Processing Consent Notice upon registration.

Upon acceptance of employment at Integrating, members of staff also consent to the processing and storage of their data.

Data must be collected and stored in a secure manner.

Personal information must not be disclosed to a third-party organisation without prior consent of the individual concerned unless the disclosure is legally required or permitted. This also includes information that would confirm whether an individual is or has been an applicant, member, or employee of Integrating.

Integrating may have a duty to disclose personal information to comply with legal or statutory obligation. The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any requests to disclose personal data should be directed to the Business Manager.

Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in

the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.

**Handling Data**

When handling, collecting, processing or storing personal data, staff and managers must ensure that:

I. all personal data is both accurate and up to date
II. errors are corrected effectively and promptly
III. data is deleted/destroyed when it is no longer needed
IV. personal data is always kept secure
V. The Data Protection Act is considered when setting up new systems or when considering use of the data for a new purpose.
VI. written contracts and agreements are used when external bodies
VII. process/handle the data explicitly specifying the above requirements with respect to the data

It is equally important not to:

I. access personal data not required for work
II. use the data for any purpose it was not explicitly obtained for
III. keep data that would embarrass or damage Integrating if disclosed (eg: via a ‘subject access’ request)
IV. transfer personal data without consent from the individual concerned or entitlement
V. store/process/handle sensitive personal data (see below) without consent or entitlement

Individuals, to whom the data relates, have the right to:

I. receive on request details of the processing relating to themselves. This includes any information about themselves including information regarding
II. the source of the data and about the logic of certain ‘fully automated decisions’
III. have any inaccurate data corrected or removed in a timely fashion
IV. stop processing data, which in certain circumstances, is likely to cause ‘substantial damage or substantial distress’
V. prevent their data being used for advertising or marketing
VI. not be subject to certain ‘fully automated decisions’ if they affect the individual

When a subject access request is received, it is important to act promptly and effectively as certain time scales are imposed regarding the response. (See Annex 1)

**Working Securely**

The Data Protection Act requires all organisations to have appropriate security to protect personal information against unlawful, or unauthorised use or disclosure and accidental loss, destruction or damage. Therefore, Integrating staff and managers will:

- keep computer passwords secure, change them regularly and not share passwords.
- lock / log off computers when away from desks
- dispose of confidential paper waste securely by shredding
- prevent virus attacks by taking care when opening emails and attachments or when visiting new websites
- work on a 'clear desk' basis – securely storing papers when not working.
- ensure visitors do not have access to areas where data is stored.
- position computer screens away from windows to prevent accidental disclosure of information.
- restrict personal data from being taken off the premises and only with the agreement of a manager
- keep a back-up of information

**Personal Data Breach**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

**Risk-assessing data breaches**

When a security incident takes place, we will quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it. The focus of risk regarding breach reporting is on the potential negative consequences for

individuals. A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. Assessment is case by case, looking at all relevant factors.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Business Manager will contact those concerned directly and without undue delay.

A ‘high risk’ means the requirement to inform individuals based on the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

**Annex 1: Subject Access Request**

A subject access request, or SAR, is a written request to a company or organisation asking for access to the personal information it holds on you.

This is a legal right everyone in the UK has, that you can exercise at any point for free in most circumstances.

The Data Protection Act 2018 (GDPR) states you can make a subject access request for free. This right of access means you can ask to review and verify the lawfulness of the processing of your personal data. For example, you might want to make a subject access request if you're not convinced the company is processing your data lawfully, or to understand what an organisation knows about you.

You might also want to ask about any logic involved in any automated decisions made about you or get confirmation that your data is being processed and request access.

GDPR gives you the right not to be subject to a decision based solely on automated processing if it affects you legally or substantively.

If you wish to make a subject access request, there is no particular format for doing so - you can simply write to or email the organisation and ask it to provide all of the information about you it is required to disclose under the Data Protection Act.

You can ask the organisation you think is holding, using or sharing your personal data to supply you with copies of your personal data.

To make a subject access request (SAR), follow these steps:

1. Make the request to the Business Manager at Integrating (see the template below)

2. Make sure you know all the information you need, so you can ask for this in the same request

3. Write to the organisation, including your full name, address and contact telephone number; any information used by the organisation to identify or distinguish you from others of the same name (account numbers, unique IDs, etc); and include details of the specific information you require and any relevant dates

4. Include a reference to the one-month deadline that applies when dealing with requests to provide personal information

5. Reference that you have the right to make a subject access request for free under the Data Protection Act 2018.

In response to your SAR, Integrating will:

1. Reply without delay and at the latest within one month, starting from the day the SAR is received.
2. Extend the period of compliance by a further two months where requests are complex or numerous, but it must inform you within one month of the receipt of the request and explain why an extension is necessary.
3. Provide you with a copy of the personal data requested in the SAR free of charge.
4. Charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
5. Charge a reasonable fee for requests of further copies of the same information, but this doesn't mean it can charge you for all subsequent access requests.
6. Provide the information in a commonly used format, but it need not do this if it is not possible, if it takes 'disproportionate effort' or if you agree to some other form, such as seeing it on screen.

| **Subject Access Request Form** | |
|---|---|
| Full Name | |
| Current address | |
| Contact number | |
| Email address | |
| Information requested | |
| ***Please tick the relevant box*** | |
| Current member of Integrating | ☐ |
| Previous member of Integrating | ☐ |
| Currently employed by Integrating | ☐ |
| Previously employed by Integrating | ☐ |
| Other – please specify | ☐ |
| ***For office use only*** | |
| ***Date request received:*** | |

| | |
|---|---|
| ***Action:*** | ***By whom:*** |