DATA PROTECTION POLICY

Version 7

JUNE 2024
To be reviewed in JUNE 2025

This policy outlines the company policy in relation to:

- Item 1
- Item 2
- Item 3
- Item 4
- Item 5

Document Control		
Version	Date	Reason Author Agreed by including date
1	June 2016	New policy
2	Feb 2017	Name change & changes to terminology
3	Apr 2018	Review to meet GDPR legislation
4	Feb 2021	Approved by trustees with plan to make further changes in 2021
5	Mar 2022	Annual review, SB & UD
6	Mar 2023	Board of trustees Meeting 25/03/2025
7	Jun 2024	Review, TR, approved by board on 08/02/25

1. Context

1.1. Integrate UK is committed to protecting the rights and privacy of individuals and needs to collect and use certain types of personal data to carry out its work, to meet its objectives and to comply with its legal obligations.

1.2. This policy sets out how we seek to protect personal data and ensure that those handling data understand the rules governing their use of the personal data to which they have access in the course of their work. This policy covers anyone who handles data on behalf of Integrate UK, including trustees, employees, volunteers and where relevant, self
employed contractors handling data on behalf of the organisation.
1.3. This document should be read in conjunction with our Safeguarding Policy and ICT Acceptable Use Agreement.

2. Definitions

Business purposes	• The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. • Business purposes include the following: • Compliance with our legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training and quality control, to administer our work with young people, our filmmaking, our trips and events and our Outreach Work. • Investigating complaints and managing Safeguarding disclosures • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments, DBS checks • Monitoring staff conduct, disciplinary matters • Applications for grants and subsequent reports to funders • Improving services • Promoting the work of the charity, events and maintaining our emailing list.

Personal data	'Personal' data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. Personal data we gather may include: an individual's phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Responsibilities

3.1. The Data Controller is Integrate UK which is overseen by the Board of Trustees who delegate the day-to-day responsibilities to the CEO as the Data Protection Lead. These responsibilities include:

a) Understanding and communicating obligations under the General Data Protection Act.
b) Identifying potential problem areas or risks
c) Producing clear and effective procedures
d) Notifying and annually renewing notification to the Information Commissioner's Office, plus notifying of any relevant interim changes.

3.2. There is no legal requirement for Integrate UK to appoint a Data Protection Officer and this should be reviewed only if there is a substantial change to data processing activities.
3.3. All Employees, Trustees, Self-employed persons and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the Guidance Notes.

4. Principles

4.1. Integrate UK shall comply with the six principles of data protection set out in the EU General Data Protection Regulations:

a) Lawful, fair and transparent: Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.
b) Limited for its purpose: Data can only be collected for a specific purpose.
c) Data minimisation: Any data collected must be necessary and not excessive for its purpose.
d) Accurate: The data we hold must be accurate and kept up to date.

e) Retention: We cannot store data longer than necessary.
f) Integrity and confidentiality: The data we hold must be kept safe and secure.

5. Policy Implementation

5.1. To comply with data protection laws and the accountability and transparency principle of GDPR, we must demonstrate compliance. To meet our responsibilities, Integrate UK employees and trustees will implement measures set out by the Board of Trustees to ensure privacy by design and default, including:

a) Ensure any personal data is collected in a fair and transparent way, and that there is a legal basis for this. This is set out in guidance notes
b) Explain why data is needed at the start. The privacy notice is in the guidance notes and privacy policy is publicly available via the website
c) Ensure the information used is necessary, accurate, up to date and no held longer than necessary. We hold an internal data map of all data processed, reviewed annually.
d) Ensure personal data is kept safely. The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Using lockable cupboards (restricted access).
- Password protection on personal information files.
- Setting up computer systems to allow restricted access to certain areas.
- Back up of data on computers (onto a separate hard drive / onto tapes kept off site).
- ICT Acceptance Use Agreement.

e) Ensure the rights people have in relation to their personal data can be exercised. An individual has the right to receive confirmation that their data is being processed, access to their personal data, and supplementary information by emailing info@integrateuk.org. How to withdraw consent or to access personal data is explained in the privacy policy on our website. Integrate UK will respond to most enquiries within 1 month, subject to checks to verify the identity of the person making the request.
f) Implement and review procedures to detect, report and investigate personal data breaches. Integrate UK is registered with the Information Commissioner's Office (ICO) and has a legal obligation to report any data breaches to the ICO within 72 hours. Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings. A Trustee could be personally liable for any penalty arising from a breach that they have made. A self-employed contractor or volunteer could have their agreement terminated for any penalty arising from a breach that they have made.

6. Review and Compliance

6.1. The Board and Trustees are accountable for compliance of this policy and to review it annually.

Guidance notes:

7. Introduction

7.1. Data Protection is a legal obligation. Anyone (including volunteers, media crew, trustees) who accesses or uses our data needs to comply with our policy and General Data Protection Act (GDPR).
7.2. These notes help us apply our policy and will be updated from time to time.

8. Your Responsibilities as employee or volunteer

8.1. Fully understand your data protection obligations.
8.2. Check that any data processing activities you are dealing with comply with our policy and are justified.
8.3. Do not use data in any unlawful way.
8.4. Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions.
8.5. Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

9. Gathering new data & checking information

9.1.We must establish a lawful basis for processing data. If you are a Data Processor (meaning you are collecting data on behalf of Integrate UK), you must first:

a) Be sure we need the data – is there another way to achieve the same outcome?
b) Check the lawful basis for any data you are working with and ensure all of your actions comply with the lawful basis. At least one of the following conditions must apply whenever we process personal data.

10. The 6 lawful bases for processing personal data

Consent: We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

Contract: The processing is necessary to fulfill or prepare a contract for the individual.

Legal obligation: We have a legal obligation to process the data (excluding a contract).

Vital interests: Processing the data is necessary to protect a person's life or in a medical situation.

Public function: Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

Legitimate interest: The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

11. Special Categories

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

a) Race
b) Ethnic origin
c) Politics
d) Religion
e) Trade union membership

f) Genetics
g) Biometrics (where used for ID purposes)
h) Health
i) Sexual orientation

In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

12. Inform

- We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose, using one of our standard privacy notices. This applies whether we have collected the data directly from the individual, or from another source.
- When submitting personal data, data subjects should be directed to our privacy policy at www.integrateuk.org/privacy-policy/.

Data Subject Rights

Individuals have a right under the Act to access certain personal data being kept about them on computers and certain files. Any person wishing to exercise this right should email info@integrateuk.org

The following information will be required before access is granted:

a) Full name and contact details of the person making the request
b) Proof of identity
c) Queries about handling personal information will be dealt with swiftly and politely. d) We will aim to comply with requests for access to personal information as soon as possible and will ensure it is provided within one month as required by the Act from receiving the written request.

Other notes

- Group emails - always put the email addresses under Bcc so they cannot be read by others who do not need this information.
- Ensure your email signature file has a link to our Privacy Policy as follows: "You can find out more about how we use your data here.
- If you don't want to hear from us anymore, email info@integrateuk.org".
- Please ensure that all email event invitations and mailing list emails communications include a Data Protection statement and link to our privacy policy.
- Paper consent forms for under 16's, and media release forms for over and under-16's with personal information go in the locked filing cabinet and some data from them is entered into our database.
- Any information relating to a safeguarding disclosure is handled securely by the CEO and Trustees as relevant.
- Printed lists of contact details and other personal information should be shredded as soon as possible. Password protect files that contain personal data and please do not share passwords to data with anyone who does not need access to this information.
- Maintain an attitude that you are responsible for someone else's property and be aware of the potential risks to Integrate UK if some or all your data was lost.

- We won't go far wrong if we get in the habit of putting ourselves in the shoes of the individual whose data we hold and ask some simple questions:
- Is the way we are using this data consistent with the reason for which it was given?
- Would the person expect us to do this, or do we need consent?
- Are we putting our own priorities above those of the individual?
- Are we taking good care of the data that has been entrusted to us?
- Would it make us feel uncomfortable if the individual concerned asked to see any of the information which we hold about them?
- Do we really need any/all of this information?