Unlocking Potential: Data Protection Policy

AMENDMENTS

Issue	Date	Author	Change Details
Version 1.0	April 2018	AF	Original Version
Version 2.0	December 2020	TT	Updated
Version 3	September 2023	TT	Updated
Version 3.1	November 2024	TT	Updated
	November 2025	AB/TT	Updated

Next Review Date: October 2026

Table of Contents

Aims and scope of this policy

Unlocking Potential (UP) is committed to protecting the personal data we process, being fully compliant with UK and EU data protection legislation and safeguarding the rights and freedoms of the people we process the data of.

In order to carry out its day-to-day operations, to meet its charitable objectives and to comply with its legal obligations, UP needs to keep certain information on its:

a. Beneficiaries (both active and archived beneficiaries)
b. Employees and contractors (including potential employees and third-party suppliers and contractors)
c. Trustees
d. Volunteers
e. Trainees and other students on placement at UP
f. Donors, supporters, sponsors and celebrity ambassadors for UP

The aim of this policy is to ensure that everyone handling personal data for and on behalf of the Charity is aware of the associated legal requirements and acts in accordance with the Charity's data protection procedures.

This policy applies to any individuals that may be authorised to access personal data on behalf of UP, such as:

a. Trustees of UP
b. Employees, workers and contractors of UP (temporary and permanent), including potential employees, agency workers and independent contractors engaged by UP
c. Volunteers engaged by UP
d. Trainees, including students on placement, engaged by UP
e. Third party data processors engaged by UP
f. All others associated with or representing UP

All these individuals are, for the purposes of this policy, associated with UP. Breach of this policy may result in:

a. For employees, trainees or volunteers - disciplinary proceedings and potential termination of employment/placement/agreement
b. For trustees – personal liability for any penalty arising from a breach they have made

UP will endeavour to ensure that:

a. Anyone who wishes to make enquiries about UP's handling of personal information, whether a member of staff, volunteer or beneficiary, understands the policies and procedures
b. Any disclosure of personal data will be in line with our procedures

c. Queries about UP's handling of personal information will be dealt with swiftly and effectively
d. Everyone processing personal data receives appropriate training in managing and processing the personal data as well as understanding what might constitute a data breach and the reporting procedure
e. Requirements to comply with this Data Protection Policy and the UK GDPR are included in Employee, Volunteer and Trainee contracts

Definitions and contacts

Data controller: 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. In this policy, Unlocking Potential are the data controller for most of the personal data.

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller e.g. our external payroll provider, processing payroll data on behalf of UP.

Data Protection Lead: is the internal member of the organisation's staff who oversees data protection obligations and procedures. Our data protection lead is Catherine Blake, for the Schools Programme and Helen Twigg for anything else.

Data Protection Officer (DPO): DPOs assist an organisation to monitor their internal compliance, inform and advise on data protection obligations, provide advice regarding data protection documents and processes and act as a contact point for data subjects and the Information Commissioner's Office (ICO). The organisation appointed Abbie Beckett from Hope & May as an external Data Protection Officer who can be contacted at abbie.beckett@up.org.uk

Data subject: refers to any living person who is the subject of personal data (see below for the definition of 'personal data') held by the organisation.

Information Commissioner's Office (ICO)*:* the UK's independent authority set up to enforce data protection law, provide guidance, uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Personal data: means any information that identifies, directly or indirectly, a data subject.

Processing: refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use,

disclosure, dissemination, combination or deletion, whether by automated means or otherwise.

Special categories of data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometric data (where used for identification purposes), data concerning health, data concerning a person's sex life or sexual orientation.

The seven principles of data protection

The UK GDPR lists the seven principles of data protection, which UP is committed to adhering to:

1. Lawfulness, fairness and transparency

UP is committed to processing data lawfully, fairly and in a transparent manner.

The charity identifies a **lawful basis** every time they start processing personal data (see section on the **six lawful bases** for more information).

UP is **transparent** about data processing, and before processing their data, informs all data subjects about the processing of their data via a privacy notice which is freely available. The organisation has created easy-read versions of the privacy notice for young people (beneficiaries under 16) to ensure information is accessible and easily understood.

Such information, as outlined above, will be provided to people as they share their data as follows:

a. For beneficiaries under 16, at the point of initial assessment and commencement of service use, via the initial assessment form, easy-read privacy notice and age-appropriate conversations

b. For the legal guardians of beneficiaries under 16, at the point of initial assessment and commencement of service use via the initial assessment form, acknowledgement letters sent home to parents or carers (coordinated by us or our school partners) and privacy notice

c. For beneficiaries over 16, at the point of initial contact and commencement of service use via an initial assessment form and privacy notice

d. For employees and potential employees, at the point of job application and commencement of service, via application forms and employment forms, as well as induction. Privacy notices will be made available at the point of application and when employment commences

e. For trustees, at the start of their term via induction training and privacy notice

f. For volunteers, at the commencements of their service, via application forms, employment forms and privacy notice, as well as induction training

g. For trainees and students on placement, at the commencement of their placement via induction training and privacy notice

h. For donors, supporters, sponsors and celebrity ambassadors, at the commencement of their support via letter, email and privacy notice

2. Purpose limitation

UP collects personal data for specified, explicit and legitimate **purposes**, and the data is not further processed in a manner that is incompatible with those purposes. The organisation may extend a purpose to cover new processing, as long as the new purpose is compatible with the old. UP will only ever collect information that is needed in order to carry out its work, meet objectives, improve services, fulfil any request that data subjects make, personalise services to best meet data subjects' needs and keep track of the impact and quality of its work.

The purposes of data processing are included in the Privacy Notice and in the Record of Processing Activity (ROPA) spreadsheet (see **demonstrating compliance** section for more information).

3 and 4. Data minimisation and accuracy

The organisation is committed to processing data that is **adequate, relevant, limited to what is necessary, accurate and kept up to date**. Data is stored in a format that is easily updated if needed. The organisation will assume that information submitted by data subjects is accurate at the date of submission, and will ensure it stays up to date with annual reviews.

All staff members are required to update the organisation as soon as reasonably possible of any changes to personal information, and the organisation keeps employee data in a HR database which is accessible and viewable by individual employees so they can check their data is up to date.

5. Storage limitation

The organisation is committed to **keeping personal data for no longer than necessary**. In some cases, retention periods will be based on legal consideration. In other cases, the reason may be more practical or based on organisational decisions. The retention schedule is logged in the ROPA spreadsheet.

The organisation shall, on an annual basis, carry out a review of all personal data held by the organisation and decide whether any data is no longer required to be held (either it

has reached its retention period or is no longer needed for the purposes that it was collected), and arrange for that data to be deleted or destroyed securely.

Should any personal data be required to be retained beyond the retention period set out in the ROPA, this may only be done with the express written approval of the Data Protection Lead/Officer, and must be in line with data protection requirements.

6. Integrity and confidentiality

The organisation ensures **appropriate security of personal data.** UP operates under a policy of confidentiality - committed to providing confidential services to beneficiaries and ensuring that all personal data about staff, trustees, volunteers and other stakeholders is treated as confidential and is collected, processed and retained in line with the data protection law. In certain situations, information may need to be shared with third parties e.g. to protect the welfare and safety of young people that are part of the service delivery.

Access to personal data is restricted to authorised groups of people within UP who will process that data. Specifically:

- **a.** Only employees, trainees or volunteers involved with a particular beneficiary, or management of a programme a beneficiary is in, safeguarding of that programme, or those involved in evaluating and monitoring that programme will have access to a particular beneficiary's personal data
- **b.** Only employees, or trustees involved with HR, finance functions, safeguarding or line management will have access to employee, trainee or volunteer data
- **c.** Only employees, trainees or volunteers involved with fundraising, commissioning or donor management will have access to donor data
- **d.** Only employees involved in trustee management or safeguarding will have access to trustee data

UP will also endeavour to ensure that the following measures are taken to keep personal data secure:

- **a.** Electronic data will be kept on encrypted servers.
- **b.** Servers will be password protected, with restricted access by employees, volunteers, trainees and students on placement.
- **c.** Any data taken off site, via laptop or USB, will be stored on an encrypted laptop or USB.
- **d.** Electronic data will be remotely backed up daily.
- **e.** Any paper-based data will be stored securely, in locked offices and locked filing cabinets. Access to keys will be restricted to staff, volunteers and students on placement where it is within their scope of authority.

f. Special categories of personal data will not be sent over non-encrypted email, except where:

- A subject access request is made
- In communications with social service providers, schools or other education provisions that may need such data on a need to know, best interest of the beneficiary basis
- In communication with mentors on a need-to-know basis, and only in the best interest basis of the beneficiary
- In communication with trusted employment partners who request this data
- In communication with partner agencies that request, and only accept, data, via 'email to fax' technology.

7. Accountability

The organisation is able to demonstrate compliance and keeps records to demonstrate the steps taken to comply with the UK GDPR:

- **Record of Processing Activities (ROPA) spreadsheet** keeps a clear record of the data the organisation processes such as the category of personal data processed for each data subject, the lawful basis of the processing, data retention, data storage, who is responsible for the data and who has access to the data
- **The breach and activity spreadsheet** keeps a log of key information such as any personal data breaches and response, notifications to the ICO, discussions and decisions about data protection, identified risks, training
- **The requests spreadsheet** logs requests to exercise any rights by data subjects or their parents, and management of those requests
- **Legitimate Interests' Assessments** (LIAs) that have been carried out
- **Data Protection Impact Assessments** (DPIAs) that have been carried out to justify the approach where processing poses particular risks
- **This Data Protection Policy** which includes most procedures relating to data protection
- **Privacy Notices** for data subjects
- **Data Processing Agreements** with data processors
- **Data Sharing Agreements** with other data controllers or joint controllers
- **Appropriate Policy Document** which may be completed in some circumstances when processing special category of data or criminal records

The organisation is registered with the ICO as it engages in the processing of personal information identifying data subjects directly or indirectly. The organisation pays an annual fee to the ICO, as required by law.

Personal data we process at Unlocking Potential

'Processing' includes obtaining, holding, amending, disclosing, destroying, deleting, sharing or otherwise using personal data, whether that information is stored electronically or in hard copy.

UP processes the following personal data about **beneficiaries**:

- **a.** Identifying details: such as names, dates of birth, family details
- **b.** Personal contact data: such as addresses and telephone numbers
- **c.** Special categories of personal data: such as information about race, ethnic origin, religion, physical and mental health or conditions (including case notes, referral forms, information about diagnosis, concerns, care plans and reviews of treatment)
- **d.** Data about communications: such as emails or phone calls received

UP processes the following personal data about **employees**:

- **a.** Identifying details: such as names, dates of birth, gender
- **b.** Personal contact data: such as addresses, telephone numbers, emails
- **c.** Employment terms and conditions
- **d.** Other personal data: such as bank account numbers, payroll information, supervision and appraisal notes, training records, qualification details
- **e.** Data about communications: such as emails or phone calls received
- **f.** Special categories of personal data: such as race, ethnic origin, politics, religion, trade union membership
- **g.** Safer Recruitment, including Criminal offence data

UP processes the following personal data about **volunteers**:

- **a.** Identifying details: such as names and dates of birth
- **b.** Personal contact data: such as addresses and telephone numbers
- **c.** Other personal data: such as bank account number, supervision and appraisal notes, training records, qualification details
- **d.** Data about communications: such as emails or phone calls received
- **e.** Safer Recruitment, including Criminal offence data

UP processes the following personal data about **trainees/placement students**:

- **a.** Identifying details: such as names, dates of birth
- **b.** Personal contact data: such as addresses and telephone numbers
- **c.** Other personal data: such as bank account numbers, supervision and appraisal notes, training records, qualification details
- **d.** Data about communications: such as emails or phone calls received
- **e.** Safer Recruitment, including Criminal offence, data

UP processes the following personal data about **trustees**:

a. Identifying details: such as names and dates of birth
b. Personal contact data: such as addresses, telephone numbers, and emails
c. Other personal data: such as professional experience

UP processes the following personal data about **donors**, **supporters**, **sponsors** and **celebrity ambassadors**:

a. Identifying details: such as names, dates of birth
b. Personal contact data: such as addresses and telephone numbers
c. Other personal data e.g. gift aid status

The lawful bases for processing personal data

UP will ensure that it has a valid basis for processing personal data and will identify which basis the personal data is processed, dependent upon the purpose and relationship with the individual. The lawful bases to process data are:

1. With the **consent** of the data subject.
If the organisation chooses consent as the lawful basis (e.g. to record counselling sessions), proof of consent will be gathered. The consent must be freely given, explicit, specific and informed. The data subject can withdraw their consent at any time.
When it comes to processing the data of minors using the lawful basis of consent, the organisation may:

- gather consent from a parent or carer
- gather consent from a local authority that acquired parental responsibility when the minor is made subject to a care order by the court
- gather the young person's consent subsequently to an assessment of competence made and documented by a relevant staff member

A young person's consent may override consent gathered from their parents or carers.

2. For a **contract** involving the data subject.
The organisation identifies contract as its lawful basis when processing is necessary for the performance of a contract to which the data subject is party (e.g. employment) or in order to take steps at the request of the data subject prior to entering a contract.

3. To meet a **legal obligation** of which the organisation is subject (e.g. sharing staff salary information with HMRC).

4. To protect personal **vital interests** (e.g. sharing someone's personal details with the ambulance service in an emergency situation)

5. To perform a task in the **public interest** or for official functions, and the task or function has a clear basis in law.

6. For the organisation's **legitimate interests** provided the data subject's interests are respected. A legitimate interests assessment is carried out by the data protection lead/officer in order to show what UP's interest is and that it is legitimate, to show why the processing is necessary in pursuing this interest, to consider potential impact on any data subjects' rights and freedoms and to measure whether the data subject might reasonably expect the organisation to process their data.

In processing criminal data or special category data (racial/ethnic origin, religious beliefs, health data, sexual orientation, political opinions, genetic/biometric data, trade union membership) UP will identify both a lawful basis for general processing from the list above, and an additional condition(s) from the Data Protection Act 2018.

The lawful bases for the different processing activities of UP are recorded in the Record of Processing Activities (ROPA) spreadsheet which is maintained and reviewed regularly.

Personal data breaches

The UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. This could include, but is not restricted to the following:

- Loss or theft of data
- Loss, theft or failure of equipment on which data is stored (e.g. laptop, memory stick or paper record)
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT systems
- Unauthorised disclosure of data
- Website defacement
- Hacking attack
- Human error
- Information being obtained by deceiving the organisation which holds it

UP has a data breach procedure which should be followed in the event of a data breach.

Data Subject Rights and Subject Access Requests

The organisation is aware of data subject rights and they are listed in our privacy notice. The data subjects' rights include:

1. **The right to be informed** about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The organisation is committed to comply with this right and do so via the privacy notice.

2. **The right of access**, data subjects have a right to access the data the organisation holds about them. UP has a Subject Access Request (SAR) procedure which explains how to recognise an incoming SAR and how the organisation must respond.

3. **The right of rectification** - if the data subject becomes aware that the organisation is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

4. **The right to be forgotten (the right to erasure)** - if a data subject asks the organisation to delete their information, the organisation will do so without undue delay when:
   - the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
   - the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing
   - the data subject objects to the processing and there are no overriding legitimate grounds for the processing
   - the personal data has been unlawfully processed
   - the personal data has to be erased for compliance with a legal obligation
   - the personal data has been collected in relation to the offer of online services to a child

   If the organisation has made the information public, the organisation must try to have it erased in other locations as well. There are some exceptions to this right, such as if the organisation has no choice but to retain the data e.g. to mark a record for suppression.

5. **The right to restrict processing** where one of the following applies:
   - the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
   - the processing is unlawful, and the data subject opposes the erasure of the personal data, requesting the restriction of its use instead
   - the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims
   - the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject

6. **The right to data portability** when processing is based on consent or a contract between the organisation and the data subject, and the processing is taking place 'by automated means', allowing data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

7. **The right to object** to any processing of their data that organisation is carrying out on the lawful basis of legitimate interests. The organisation will stop processing if not able to demonstrate 'compelling legitimate grounds'.

8. Rights in relation to **automated decision making and profiling**

Some additional rights of data subjects include:

- The right not to receive direct marketing
- The right to claim damages should they suffer any loss as a result of a personal data breach
- The right to complain and the right to request that the ICO carry out an assessment of the processing of the organisation, although they should make their complaint to the organisation in the first instance.

If you believe a data subject has made one of the above requests, you must forward this on to the data protection lead who will liaise with the Data Protection Officer on how to respond.

Data sharing and working with other organisations

If you need to share personal data to an organisation outside of UP, you must ensure you have the consent of the data subject, or if this isn't appropriate, ensure UP has an agreement or contract with the other organisation. Reach out to the data protection lead who can advise.

All third parties we work with who have or may have access to personal data of our data subjects will either comply with this policy, or we will ensure that their data protection policy aligns with this policy.

If we work with organisations who will act as data processors (who will process data on behalf of UP) we will ensure they are compliant with data protection legislation by entering into a Data Processor Agreement, or ensuring out contract includes obligations relating to data protection. Where we collaborate with separate data controllers and share data, we may agree to a Data Sharing Agreement.

We do not transfer individuals' personal data outside of the UK, EU or EEA. We must apply safeguards if we were to transfer data internationally.

Training and awareness

Training about data protection in this organisation will take the following forms:

Induction training

All employees, trainees/placement students, volunteers and trustees undergo induction training regarding data protection and this policy. At this induction, all participants are asked

to confirm that they understand this policy and will receive a copy of it for their future reference.

Training for those whose role involves extensive data processing

Any employees, trainees, volunteers or trustees whose scope of authority includes extensive data processing, including programme leaders and evaluation staff, will undergo more extensive training around data protection. Such training will be updated regularly and as needed in accordance with changing Data Protection Regulation, best practice and UP's learning and experience.

UP will also make employees, trainees, volunteers and trustees aware of data protection requirements through various forms, such as: posters outlining data protection requirements, annual email updates etc.

Review

This policy will be reviewed as required by the data protection lead and officer to ensure it remains up to date and compliant with the law.

If you believe that the charity has not complied with your data protection rights, you can file a complaint with the Information Commissioner at https://ico.org.uk/global/contact-us/