Data Protection Policy

CONTENTS

Reviewed:	April 2018
Reviewer:	AFR
Approved:	May 2018

AIMS

UP – Unlocking Potential (UP) is committed to the protection of personal data, including special categories of personal data (previously referred to as personal sensitive data) and criminal allegations, proceedings and conviction in accordance with EU General Data Protection Regulation 2018 (GDPR). GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. The GDPR applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. In this instance UP-Unlocking Potential is a controller responsible for the processing of personal data and also determines 3rd party organisations to act as a processor, e.g. the external payroll provider.

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 Charity is committed to ensuring any personal data will be processed in compliance with the GDPR. In summary, this means that UP's policy is for personal information to be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

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:

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; and

f. All others associated with or representing UP.

All these individuals are, for the purposes of this policy, associated with UP.

CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL DATA

In line with the GDPR, UP will ensure that personal data shall be processed lawfully, fairly and in a transparent manner. 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 for processing personal data are as follows:

a. The data subject has given consent to the processing of their personal data for one or more specific purposes; or

b. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

c. Processing is necessary for compliance with a legal obligation to which the controller is subject; or

d. Processing is necessary to protect the vital interests of the data subject or of another person; or

e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

f. Processing is necessary for the purposes of the legitimate interest pursued by the controller. This will require the controller to:

- Identify a legitimate interest
- Show that the processing is necessary to achieve it, and
- Balance it against the individual's interests, rights and freedoms

In processing special category data, UP will identify both a lawful basis for general processing and an additional condition for processing this type of data.

In processing criminal conviction data or data about offences, UP will identify both a lawful basis for general processing and an additional condition for processing this type of data.

PROCESSING OF PERSONAL DATA

'Processing' includes obtaining, holding, amending, disclosing, destroying, deleting 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;

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.

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.

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;

f. 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 and telephone numbers;

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: such as bank account numbers.

Access to the personal data for which UP is responsible will be 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.

We are currently registered with the Information Commissioner and our current registration reference is: ZA150080.

The name of the Data Protection Officer and contact for data protection matters within our organisation as specified in our notification to the Information Commissioner is Avalon French.

RESPONSIBILITIES FOR DATA PROTECTION COMPLIANCE

Overall responsibility for the Charity's data protection compliance falls to the Board of Trustees.

The Board of Trustees delegates particular responsibilities and tasks regarding data protection to the Chief Executive Officer who, in turn, delegates responsibilities to the Data Protection Officer.

The Data Protection Officer is responsible for:

a. understanding, communicating and advising obligations to comply with GDPR and other data protection laws;

b. monitoring compliance with the GDPR and other data protection laws and with UP's data protection policies, including managing internal data protection issues, training employees and conducting internal audits;

c. advice on and monitoring of data protection impact assessments;

d. co-operating with the supervisory authority; and

e. being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, beneficiaries, etc).

All employees, volunteers, trainees, placement students, trustees and third-party data processors who process personal information must ensure they not only understand but also act in line with this policy and the GDPR.

Breach of this policy may result in:

a. for employees, trainees or volunteers - disciplinary proceedings and potential termination of employment/agreement;

b. for trustees - potentially personally liable for any penalty arising from a breach they have made.

All employees, trainees, volunteers, trustees and third-party data processors who identify, or suspect, a data breach must report this breach the Data Protection Officer or the CEO in their absence.

Where a data breach is reported or suspected, UP will put in place a crisis management plan to evaluate the nature, scope and potential consequences of the breach. This will be led by the CEO.

Where UP has assessed that a breach is of an appropriate nature, i.e. likely to result in a high risk to people's rights and freedoms or consequences, we will notify:

a. the appropriate regulatory bodies, including the Information Commissioner within 72 hours of first having become aware of the breach;

b. those individuals affected by this breach without undue delay after first becoming aware of a data breach. This will include a description of the breach and how and when it occurred, our responses to the risks the breach posed, clear and specific advice around what they can do to minimise their risks, and information on how to contact us further.

The Charity will then investigate the causes of the breach and evaluate our effectiveness of response, with a view to minimise ongoing risks.

POLICY IMPLEMENTATION

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 GDPR are included in Employee, Volunteer and Trainee contracts.

TRAINING AND RAISING AWARENESS

Training about GDPR and how it is followed in this organisation will take the following forms:

a. 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.

b. 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.

ENSURING COMPLIANCE WITH THIRD-PARTY DATA PROCESSORS

Where data is processed by third-party data processors, they will also be bound by this policy.

UP will work with only those third-party data processors who are able to provide sufficient guarantees in respect of the technical security measures and organisational measures governing the data processing to be carried out in line with GDPR.

UP will ensure that all third-party data processing will be governed by a contract stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the Data Protection Act and GDPR to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing.

COLLECTIING DATA, STORING DATA AND CONSENT TO USE OF PERSONAL DATA

Before personal data is collected individuals will be provided with privacy information including:

- UP's purposes for processing their personal data;
- Retention periods for that personal data;
- Who it will be shared with.

UP will consider the following:

a. The extent of the details that are necessary for our purposes;

b. Our legal obligations under safeguarding legislation and guidance;

c. How long we are likely to need, and keep, this information;

d. Who should have access to this information, and the means to process it that will ensure such restricted access;

e. Implementing appropriate technical and organisational measures in an effective way in order to meet the requirements of this regulation and protect the rights of data subjects;

f. Ensuring that all consent for data is freely given, specific, informed, unambiguous and separate from other terms and conditions;

g. Providing a positive opt–in consent that is not inferred through silence or inactivity.

UP will inform people whose data is gathered about the following in concise, easy to understand and clear language:

a. Why we are gathering the data and our lawful basis for processing the data;
b. What the data will be used for;
c. Who will have access to the data;
d. How long UP will retain the data.
e. The right to complain to the ICO if they think there is a problem with the way UP is handling their data.

If asked, UP will provide a copy of the personal data, free of charge, in an electronic format.

Where UP is gathering information about beneficiaries who are under 16, both beneficiaries and their legal guardians will be informed about:
a. Why we are gathering the data;
b. What the data will be used for;
c. Who will have access to the data.

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 their initial assessment forms 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:
i. their initial assessment form;
ii. consent letters sent home to parents or carers (which may be coordinated by us or our school partners).
c. For beneficiaries over 16, at the point of initial contact and commencement of service use via an initial assessment form.
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.

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

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

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

Data about employees, volunteers, and trustees' DBS checks, and other criminal records/barring list updates, will be updated annually by UP's HR department. Records about updates will be recorded securely on an electronic database.

Data about trainees' DBS checks, and other criminal records/barring list updates, will not be updated unless they work with us for more than 1 year. In this case, details will be updated on a secure electronic database. In the event that they transfer on to becoming a volunteer or employee, this responsibility will move to the HR department.

Beneficiaries

UP will take the following measures to ensure that active beneficiaries' personal data is kept accurate by assigning designated members of staff to routinely update such information.

Consent to use active beneficiaries' personal data on an on-going basis, i.e. for as long as the beneficiary is accessing UP Services, is normally secured at the start of each beneficiary's contact with our Services.

For archived (i.e. non-active) beneficiaries, their data will be archived at the end of their relationship with UP. Employees responsible for the decision to close beneficiary cases will be tasked with ensuring all data is accurate at the point of archiving. No attempt will be made to ensure data is kept up to date after the point of archiving, save for the event that a beneficiary actively returns to use an UP service.

a. Archived data will be stored on our encrypted database for 10 years, or until the beneficiary reaches 30 years old, whichever comes first. This is to ensure that potentially vital health and social care records remain available for a reasonable amount of time. All

paper-based files will be transferred on to our database and then securely destroyed at the point where a beneficiary is archived.

b. Data relating to safeguarding concerns, or beneficiaries who had significant safeguarding concerns, will be archived indefinitely.

Consent to use archived beneficiaries' personal data will be sought each specific time their data is to be used. For archived beneficiaries who are under 16 at the time of the proposed use of their personal data, both the archived beneficiary and the archived beneficiary's parent/carer will be asked to consent beforehand.

a. Where both the parent/carer and beneficiary consent, the data will be processed.

b. Where the parent/carer consents but beneficiary does not consent, a Designated Safeguarding Lead at UP will make contact with the beneficiary to assess their capacity to consent to such a request.

i. Where the Designated Safeguarding Lead is assured the beneficiary does not have the capacity to consent, and processing the data poses no potential harm to their wellbeing, the data will be processed in accordance with their legal guardian's consent.

ii. Where the Designated Safeguarding Lead is assured the beneficiary does not have the capacity to consent, but disclosing the data requested poses some potential harm to their wellbeing, the request will be escalated as a safeguarding concern, in order to balance UP's obligation to safeguard children with the need to process data and their legal guardian's consent.

iii. Where the Designated safeguarding Lead is assured the beneficiary has the capacity to consent, the data will not be processed in accordance with their wishes.

c. Where the beneficiary consents but the legal guardian does not consent, a Designated Safeguarding Lead at UP will make contact with the beneficiary to assess their capacity to consent to such a request:

i. Where the Designated Safeguarding Lead is assured the beneficiary does not have the capacity to consent, the data will not be processed in accordance with their legal guardian's consent.

ii. Where the Designated Safeguarding Lead is assured the beneficiary has the capacity to consent, and processing the data poses no potential harm to their well-being, the data will be processed in accordance with their wishes.

iii. Where the Designated Safeguarding Lead is assured the beneficiary has the capacity to consent, but processing the data requested poses some potential harm to their well-being, the request will be escalated as a safeguarding concern, in order to balance UP's obligation to safeguard children with the need to process data and their wishes.

d. Where neither beneficiary nor parent/carer consents, the data will not be processed.

Employees

UP will ensure that current employees' personal data is kept accurate by ensuring that all personal data is stored on the HR database which is accessible and viewable by the individual employee.

Former employees who have left employment at UP will keep necessary data, such as contact details, start and termination dates, salary levels and supervision and appraisal notes securely on an encrypted database for 6 years from the termination of employment. Bank details will be deleted/destroyed 3 months after the termination of employment. Other personal data will be destroyed 6 years after the employment has ended unless there is a contractual or legal basis for retaining longer than 6 years.

Volunteers

UP will ensure that active volunteer personal data is kept accurate by the Volunteer Manager.

For volunteers who are no longer working with the charity, UP will keep necessary data (such as contact details, start and termination dates and supervision notes) securely on an encrypted database for 6 years from the date of leaving, unless there is a legal basis for retaining the data for longer than 6 years. Bank details (if recorded for a volunteer) will be deleted or destroyed 3 months after their volunteering relationship has ended with the charity.

Trainees & Students

UP will ensure that active the personal data of trainees and students on placement with us is kept accurate an up to date.

For trainees and students on placement with us, UP will keep necessary data (such as contact details, start and termination dates, supervision and appraisal notes) securely on an encrypted database for 6 years from the date they leave, unless there is a legal basis for retaining longer that data for than 6 years. Bank details (if recorded for a trainee/student) will be deleted or destroyed 3 months after the placement with the charity has ended.

UP will ensure that active trustees' personal data is kept accurate and up to date.

Trustees

For previous trustees, UP will keep necessary data (such as start and termination dates) securely on an encrypted database for 6 years from the date they cease being a trustee, unless there is a legal basis for retaining that data for longer than 6 years. Bank details (if recorded for a trustee) will be deleted/destroyed 3 months after the cessation of their trusteeship with UP.

Donors, etc.

UP will ensure that active donors, supporters, sponsors and celebrity ambassador's personal data is kept accurate through annual reviews.

For previous donors, supporters, sponsors and celebrity ambassadors, UP will keep necessary data (such as donations and contact details) securely on an encrypted database for 6 years. Bank details (if recorded) will be deleted or destroyed 3 months after their last donation, sponsorship or ambassadorship.

DATA SECURITY

UP will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. UP will endeavour to ensure that the following measures are taken:

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. 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.

f. 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 the scope of their authority.

SUBJECT ACCESS REQUESTS AND THEIR AUTHORISATION

Individuals have a right under the GDPR to access certain personal data being kept about them on computer and other files. They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, object or restrict the processing of their data, block or erase their information.

Beneficiaries also have the right to receive the personal data concerning them, which they have previously provided, in a common use and machine-readable format, and have the right to transmit that data to another controller under the following conditions:

i. personal data that an individual has provided to a controller;

ii. where the processing is based on the individual's consent for the performance of a contract;

iii. when processing is carried out by automated means.

All persons, except active beneficiaries, wishing to exercise these rights should either:

a. apply in writing to:

The Data Protection Officer, UP–Unlocking Potential, Larcom House, 9 Larcom Street SE17 1RX;

b. apply via email to: dpo@up.org.uk; or

c. apply via telephone by calling: 020 3450 3550.

The following information will be required before access is granted to individuals, except for individuals who are active beneficiaries:

a. Full name and contact details of the person making the request;

b. Their relationship with UP, e.g. former beneficiary, current volunteer etc.;

c. Information relevant to the request, such as timescales involved, or types of data required.

We may also require proof of identity before access is granted to individuals, except for individuals who are active beneficiaries. For subject access requests regarding non-sensitive personal data, the data subject will need to confirm all of:

a. Full name;

b. Date of birth (except for trustees and donors, where we will not collect this data);

c. Postal address, as last known by UP;

d. Contact number, as last known by UP;

e. Nature of their relationship with UP, e.g. current/former beneficiary, of which service, rough timescales etc.;

Where these requirements cannot be met, or where the request is regarding sensitive personal data, the following forms of ID may be required before data is disclosed:

a. Photographic driver's licence;

b. Passport; or

c. Birth certificate and current utility bill / council tax bill / bank statement.

Active (i.e. non-archived) beneficiaries wishing to exercise their subject access rights should contact their designated staff member in the first instance. Where they would rather make the request to someone else, they can contact the Data Protection Officer by via post, email or telephone:

a. The Data Protection Officer, UP–Unlocking Potential, Larcom House, 9 Larcom Street SE17 1RX;

b. dpo@up.org.uk;

c. 020 3450 3550.

The following information will be required before access is granted to individuals who are active (i.e. non-archived) beneficiaries:

a. Full name and contact details of the person making the request

b. Information relevant to the request, such as timescales involved or types of data required.

For active (i.e. non-archived) beneficiaries, their designated staff member will confirm their identity directly.

Where a Subject Access Request is made by an active or an archived beneficiary, who is at the time of the request under 16 years old, a Designated Safeguarding Lead of UP will make contact with the beneficiary to assess their capacity to understand the consequences of such a request.

a. Where the Designated Safeguarding Lead is assured that they have the capacity, the Subject Access Request will be responded to as above.

b. Where the Designated Safeguarding Lead is not assured they have the capacity, but disclosing the data requested poses no potential harm to their wellbeing, the Subject Access Request will be responded to as above.

c. Where the Designated Safeguarding Lead is not assured they have the capacity, and disclosing the data requested poses some potential harm to their wellbeing, the subject will be encouraged and supported to make the request alongside their legal guardian.

d. Where the Designated Safeguarding Lead is not assured they have the capacity, and disclosing the data requested poses some potential harm to their wellbeing, and the subject does not wish to make the request alongside their legal guardian, the request will be escalated as a safeguarding concern, in order to balance their right to their data and UP's obligation to safeguard children.

Where a subject access request is made about an active beneficiary, or an archived beneficiary, who is at the time of the request under 16, by their legal guardian, a Designated Safeguarding Lead at UP will make contact with the beneficiary to assess the capacity understand the consequences of to such a request.

a. Where the Designated Safeguarding Lead is assured the beneficiary does not have the capacity to consent, but disclosing the data requested poses no potential harm to their wellbeing, the Subject Access Request will be responded to as above.

b. Where the Designated Safeguarding Lead is not assured the beneficiary has the capacity to consent, but disclosing the data requested poses some potential harm to their wellbeing, the request will be escalated as a safeguarding concern, in order to balance their right to their data and UP's obligation to safeguard children.

c. Where the Designated Safeguarding Lead is assured the beneficiary has the capacity to consent, the guardian will be encouraged and supported to make the request alongside the beneficiary.

d. Where the Designated Safeguarding Lead is assured the beneficiary has the capacity to consent, and the guardian does not wish to make the request alongside the beneficiary, the request will be escalated as a safeguarding concern, in order to balance their right to their data and UP's obligation to safeguard children.

Subject Access Requests about active beneficiaries, or archived beneficiaries, who are at the time of the request 16 years or older, will not be accepted from their legal guardians. Any legal guardians making such a request will be encouraged to make the request

alongside the beneficiary. Where the guardian suggests that the beneficiary is unable to consent, the request will be escalated as a safeguarding concern, in order to balance their subject access rights and UP's obligation to safeguard children and 'at risk' adults. The safeguarding concern process will always involve an assessment of the beneficiary's ability to consent to a subject access request themselves.

In all instances where a Subject Access Request is deemed appropriate, data will be returned to individuals in an appropriate, secure format within a month's time. The preferences of the data subject themselves will be given due consideration, but generally:

a. Our preference is to send data via encrypted emails where the subject has the ability to confirm encrypted messages and receive them.

b. Where the subject does not have this capacity, we will send out hard copies of data or for large files, an encrypted USB, either handed over in person or sent via recorded mail.

c. Where a subject requests data to be sent via non-encrypted emails, we seek written (via email) confirmation of this request and explicit acknowledgement that they understand the risks of such request, before complying.

In instances where a subject access request is denied, we will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy without undue delay within a one-month time frame.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within one month of receiving the request, as required by GDPR.

REVIEW

This policy will be reviewed annually 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/.