GDPR Data Protection Policy	
Data Controller's Name:	**Positive Youth Foundation**
Data Controller's Address:	**The Techno Centre Coventry University Technology Park Puma Way Coventry CV1 2TT**
Name of Person with Responsibility for Data Protection	**Julie Kinley | Director of Business Services**
Telephone No:	**02476 158550**
Email Address:	**julie@positiveyouthfoundation.org**

GDPR Data Protection Policy Sign Off This GDPR Data Protection Policy was Reviewed, Approved & Adopted as follows:	
Date Review Undertaken:	**23rd July 2026**
Review Undertaken By:	**Julie Kinley | Director of Business Services**
Date of Adoption:	**27th July 2026**
Date of Next Review:	**27th July 2027**
Signed Off By:	**Rashid Bhayat | CEO**

GDPR Data Protection Policy Index

Definitions

In this data protection policy, the following words and phrases have the following meanings:

- **Consent** | means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

- **Criminal Records Personal Data** | means personal data relating to criminal convictions and offences and personal data relating to criminal allegations and proceedings.

- **Data Protection Legislation** | means the UK **General Data Protection Regulation (GDPR)**, the **Data Protection Act 2018** and any other applicable primary or secondary legislation as may be in force in the UK from time to time.

- **Data Subject** | means a living identified or identifiable individual about whom the organisation holds personal data.

- **Staff** | is any director (which also refers to any trustee or non-executive director, where relevant to the organisation), employee, worker, agency worker, apprentice, intern, volunteer, contractor and consultant employed or engaged by the organisation.

- **Personal Data** | is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data **i.e.** where all identifying particulars have been removed.

- **Processing** | is 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 collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

- **Job Applicant** | is any person that applies for any paid or non-paid role with the organisation.

- **Special Categories of Personal Data** | means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject's sex life or sexual orientation.

Introduction

This policy sets out how the organisation processes the personal data of data subjects, including the personal data of job applicants and the personal data of its current and former staff, clients, customers, suppliers and other third parties. It applies to all personal data that the organisation processes, regardless of the media on which those personal data are stored **e.g.** electronically, on paper or on other materials. The organisation is committed to being clear and transparent about how it collects and uses personal data and to complying with its data protection obligations.

Protecting the confidentiality, security and integrity of the personal data that the organisation processes is also of paramount importance to its business operations.

The organisation will process personal data relating to you in accordance with this policy, the data protection legislation and the latest privacy notice which has been issued to you.

This policy applies to all members of staff. It is non-contractual and does not form part of any employment contract, engagement agreement, or any other contract for services.

As a member of staff, you are yourself a data subject and you may also process personal data on the organisation's behalf about other data subjects. This policy should therefore be read and interpreted accordingly. You must always comply with it when processing personal data on the organisation's behalf in the proper performance of your job duties and responsibilities. The data protection legislation contains important principles affecting personal data relating to data subjects. The purpose of this policy is to set out what the organisation expects from you and to ensure that you understand and comply with the rules governing the processing of personal data to which you may

have access in the course of your work - so as to ensure that neither the organisation nor you breach the data protection legislation.

The organisation takes compliance with this policy very seriously. Any breach of this policy - or any breach of the data protection legislation - will be regarded as misconduct and will be dealt with under the organisation's Disciplinary Procedure. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (or procuring their disclosure to a third party) without the organisation's consent, constitutes a gross misconduct offence and could lead to your summary dismissal. If you are not an employee, you may have your contract with the organisation terminated with immediate effect.

Person with responsibility for data protection

The organisation has appointed a person with responsibility for our data protection compliance. You should contact the person with responsibility for data protection - named at the beginning of this document - if you have any questions about the operation of this policy or you need further information about the data protection legislation, or if you have any concerns that this policy is not being or has not been followed. You must also contact them to seek further advice in the following circumstances:

- If you are in any doubt about what you can or cannot disclose and to whom
- If you are unsure about the lawful basis you are relying on to process personal data
- If you need to rely on consent to process personal data
- If you need to obtain or issue privacy notices
- If you are not clear about the retention period for the personal data being processed
- If you are unsure about what appropriate security measures you need to implement to protect personal data
- If you need assistance in dealing with any rights invoked by a data subject
- If you suspect there has been a personal data breach
- Where you propose to use personal data for purposes other than that for which they were collected
- Where you intend to engage in a significant new or amended data processing activity
- Where you plan to undertake any activities involving automated decision-making, including profiling
- If you need assistance with, or approval of, contracts in relation to sharing personal data with third-party service providers
- If you believe personal data are not being kept or deleted securely or are being accessed without the proper authorisation
- If you suspect there has been any other breach of this policy or any breach of the data protection principles.

If you wish to make an internal complaint that this policy is not being - or has not been - followed, you can also raise this as a formal grievance under the organisation's Grievance Procedure (where you are an employee), or via the relevant complaints process applicable to your engagement with the organisation (where you are not an employee).

The Data Protection Principles

Under the data protection legislation, there are six data protection principles that the organisation and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness**, **fairness** and **transparency**).

2. Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**).

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**).

4. Accurate and, where necessary, kept up to date; every reasonable step must also be taken to ensure that personal data that are inaccurate - having regard to the purposes for which they are processed - are erased or rectified without delay (**accuracy**).

5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (**storage limitation**).

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

The organisation is responsible for - and must be able to demonstrate compliance with - these data protection principles. This is called the Principle of Accountability.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle means that both the organisation and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

Lawfulness and fairness | **The data protection legislation provides that processing is only lawful in certain circumstances. These include where:**

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- The processing is necessary for the performance of a contract with the data subject **e.g.** an employment contract, or in order to take steps at the request of the data subject prior to entering into a contract
- The processing is necessary for compliance with the organisation's legal obligations
- The processing is necessary to protect the data subject's vital interests (or someone else's vital interests)
- The processing is necessary to pursue the organisation's legitimate interests (or those of a third party), where the data subject's interests or fundamental rights and freedoms do not override the organisation's interests; the purposes for which the organisation processes personal data for legitimate interests must also be set out in an appropriate privacy notice.

The organisation and members of staff must only process personal data on the basis of one or more of these lawful bases for processing. Before a processing activity starts for the first time - and then regularly while it continues - the organisation will review the purpose of the processing activity, select the most appropriate lawful basis (or bases) for that processing and be satisfied that the processing is necessary for the purpose of that lawful basis (or bases). When determining whether the organisation's legitimate interests are the most appropriate basis for lawful processing, the organisation will conduct a legitimate interests assessment, keep a record of it and keep it under review.

Where the organisation relies on consent as the lawful basis for processing, this requires the data subject to have given a positive statement, active opt-in or clear affirmative action.

*** Pre-ticked boxes, inactivity or silence do not constitute consent ***

If consent is given in a document that also deals with other matters, the request for consent must be clearly distinguishable and kept separate from those other matters. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, so you must ensure that you obtain separate consents for different types of processing, where appropriate. Data subjects also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

The data protection legislation also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies (this is an additional requirement; the processing must still meet one or more of the conditions for processing set out above). These include where:

- The data subject has given their explicit consent to the processing of their personal data for one or more specified purposes - such explicit consent requires a very clear and positive statement and it cannot be implied from the data subject's actions
- The processing is necessary for the purposes of carrying out obligations or exercising specific rights of either the organisation or the data subject under employment law or social security law
- In the case of special categories of personal data, the processing relates to personal data which are manifestly made public by the data subject
- The processing is necessary for the establishment, exercise or defence of legal claims.

The organisation may from time to time need to process special categories of personal data and criminal records personal data. The organisation and members of staff must only process special categories of personal data and criminal records personal data where there is also one or more of these additional lawful conditions for processing. Before processing any special categories of personal data and criminal records personal data, you must notify the

person responsible for data protection within the organisation, so that they may assess whether the processing complies with one or more of these additional lawful conditions.

A clear record must be kept of all consents - including explicit consents - which covers what the data subject has consented to, what they were told at the time and how and when consent was given. This enables the organisation to demonstrate compliance with the data protection requirements for consent.

Transparency | Under the data protection legislation, the transparency principle requires the organisation to provide specific information to data subjects through appropriate privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. Privacy notices may comprise general privacy statements applicable to a specific group of data subjects **e.g.** staff, or they may be stand-alone privacy statements covering processing related to a specific purpose.

Whenever the organisation collects personal data directly from data subjects - including for employment purposes - the organisation must provide the data subject with all the information required to be included in a privacy notice. This includes:

- The identity and contact details of the organisation (as **Data Controller**) and any representative
- Where applicable, the identity and contact details of the person responsible for data protection
- The purposes for which the personal data will be processed
- The lawful basis or bases for processing
- Where the organisation are relying on our legitimate interests (or those of a third party) as the lawful basis for processing, what those legitimate interests are
- The categories of personal data, unless they were obtained directly from the data subject
- The third-party sources that the personal data originate from, unless they were obtained directly from the data subject
- The recipients, or categories of recipients, with whom the personal data may be shared
- Details of transfers to third countries or international organisations and the suitable safeguards applied
- The retention period for the personal data or - if that is not possible - the criteria to be used to determine the retention period
- The existence of the data subject's rights **i.e.** subject access, rectification, erasure, restriction of processing, objection and data portability
- The right to withdraw consent to processing at any time, where consent is being relied on as the lawful basis for processing
- The right to lodge a complaint with the **Information Commission**
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation, or a requirement necessary to enter into a contract, and the possible consequences of failing to provide the personal data
- The existence of any automated decision-making, including profiling, and meaningful information about how decisions are made, the significance and consequences.

The organisation must issue a privacy notice, which can be by electronic means, when the organisation first collects a data subject's personal data from them. If the personal data have been obtained from third parties, the organisation must provide the privacy notice information within a reasonable period of having obtained the personal data, but at the latest **within one month**.

However, if the personal data are to be used to communicate with the data subject, the privacy notice information is to be provided, at the latest, when the first communication takes place, or if disclosure of the personal data to another recipient is envisaged, it is to be provided, at the latest, when the data are first disclosed.

You must comply with these rules on privacy notices when processing personal data on the organisation's behalf in the proper performance of your job duties and responsibilities.

The organisation will issue privacy notices to you from time to time and these can also be obtained from the person with responsibility for data protection, named at the beginning of this document.

Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes.

Personal data cannot be used for new, different or incompatible purposes from those disclosed to the data subject when they were first obtained, for example in an appropriate privacy notice, unless the data subject has been

informed of the new purposes and the terms of this policy are otherwise complied with **e.g.** there is a lawful basis for processing. This also includes special category personal data and criminal records personal data.

Data minimisation

Personal data must be **adequate**, **relevant** and **limited** to what is necessary in relation to the purposes for which they are processed.

The organisation will only collect personal data to the extent that they are required for the specific purposes notified to the data subject. You must only process personal data where your job duties and responsibilities require it and you must not process personal data for any reason which is unrelated to your job duties and responsibilities. In addition, you must ensure that any personal data you collect are adequate and relevant for the intended purposes and are not excessive. This includes special category personal data and criminal records personal data.

When personal data are no longer needed for specified purposes, you must ensure that they are destroyed, erased or anonymised in accordance with the organisation's rules on data retention and destruction set out below.

Accuracy

Personal data must be **accurate** and, where necessary, **kept up to date**. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

It is important that the personal data that the organisation hold about you as a data subject is accurate and up to date. Please keep the organisation informed if your personal data changes **e.g.** you change your home address, so that records can be updated. The organisation cannot be held responsible for any errors in your personal data in this regard unless you have notified the organisation of the relevant change. The organisation will promptly update your personal data if you advise the organisation that the information has changed or is inaccurate.

You must also ensure that the personal data that the organisation hold about other data subjects is accurate and up to date where this is part of your job duties or responsibilities. This includes special category personal data and criminal records personal data. You must check the accuracy of any personal data at the point of their collection and at regular intervals thereafter. You must take all reasonable steps to destroy, erase or update outdated personal data and to correct inaccurate personal data.

Storage limitation

Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

The organisation will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed - including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes special category personal data and criminal records personal data. You must comply with the organisation's rules on data retention and destruction set out below.

Retention of data relating to job applicants

If a job applicant's application for employment or engagement is unsuccessful, the organisation will generally hold their personal data, including special category personal data and criminal records personal data, for six months after the end of the relevant recruitment exercise but this is subject to:

a) Any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records.

b) The retention of some types of personal data for up to **six years** to protect against legal risk **e.g.** if they could be relevant to a possible legal claim in a **Tribunal**, **County Court** or **High Court**.

If the job applicant has consented to the organisation keeping their personal data on file **e.g.** in case there are future suitable opportunities with the organisation, then the organisation will hold their personal data for a further **12 months** after the end of the relevant recruitment exercise, or until they withdraw their consent if earlier.

Retention of data relating to members of staff

The organisation will generally hold personal data, including special category personal data and criminal records personal data, for the duration of a member of staff's employment or engagement. The exceptions are:

- Any personal data supplied as part of the recruitment process will not be retained if they have no bearing on the ongoing working relationship
- Criminal records personal data collected in the course of the recruitment process will be deleted once they have been verified through a **DBS** criminal record check, unless, in exceptional circumstances, the information has been assessed by the organisation as relevant to the ongoing working relationship
- It will only be recorded whether a **DBS** criminal record check has yielded a satisfactory or unsatisfactory result, unless - in exceptional circumstances - the information in the criminal record check has been assessed by the organisation as relevant to the ongoing working relationship
- If it has been assessed as relevant to the ongoing working relationship, a **DBS** criminal record check will nevertheless be deleted after **six months** - or once the conviction is **spent**, if earlier - unless information about spent convictions may be retained because the role is an excluded occupation or profession
- Disciplinary, grievance and capability records will only be retained until the expiry of any warning given - but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment
- Negative or normal temperature or other medical testing or screening results **e.g.** coronavirus or other pandemic viruses - will either not be recorded at all or will be retained for no longer than **one week** and positive or abnormal temperature or other medical testing or screening results will be retained for no longer than **21 days**.

Once a member of staff has left employment - or their engagement has been terminated - the organisation will generally hold their personal data, including special category personal data and criminal records personal data, for 12 months after the termination of their employment or engagement, but this is subject to:

a) Any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records.

b) The retention of some types of personal data for up to **six years** to protect against legal risk **e.g.** if they could be relevant to a possible legal claim in a **Tribunal**, **County Court** or **High Court**.

c) The organisation will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for up to **six years** after the termination of their employment or engagement.

Overall, this means that the organisation will **thin the file** of personal data that is held on members of staff **12 months** after the termination of their employment or engagement, so that the organisation will only continue to retain for a longer period what is strictly necessary.

Retention of data relating to other third parties

The organisation will generally hold personal data, including special category personal data and criminal records personal data, belonging to clients, customers and suppliers for the duration of the organisation's business relationship with them.

Once the business relationship with a client, customer or supplier has been terminated, the organisation will generally hold their personal data, including special category personal data and criminal records personal data, for 12 months after the termination of the business relationship, but this is subject to:

a) Any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records.

b) The retention of some types of personal data for up to **six years** to protect against legal risk **e.g.** if they could be relevant to a possible legal claim in a **County Court** or **High Court**.

Overall, this means that the organisation will **thin the file** of personal data that is held on clients, customers and suppliers **12 months** after the termination of the business relationship, so that the organisation will only continue to retain for a longer period what is strictly necessary.

Destruction and erasure

All personal data, including special category personal data and criminal records personal data, must be reviewed before destruction or erasure to determine whether there are special factors that mean destruction or erasure should be delayed. Otherwise, they must be destroyed or erased at the end of the retention periods outlined above.

If you are responsible for maintaining personal data - and are not clear what retention period should apply to a particular record - please obtain further guidance and advice from the person with responsibility for data protection, named at the beginning of this document.

Personal data which are no longer to be retained will be permanently erased from the organisation's IT systems or securely and effectively destroyed **e.g.** by cross-shredding of hard copy documents, burning them or placing them in confidential waste bins or by physical destruction of storage media, and the organisation will also require third parties to destroy or erase such personal data where applicable.

You must take all reasonable steps to destroy or erase personal data that the organisation no longer requires.

In some circumstances, the organisation may anonymise personal data so that they no longer permit a data subject's identification. In this case, the organisation may retain such personal data for a longer period.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The organisation takes the security of personal data seriously and has implemented and maintained safeguards which are appropriate to the size and scope of the business, the amount of personal data that the organisation holds and any identified risks. This includes encryption and pseudonymisation of personal data where appropriate. The organisation have also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of the organisation's processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner. The organisation regularly test and evaluate the effectiveness of its technical and organisational safeguards to ensure the security of the organisation's processing activities.

In turn, you are responsible for protecting the personal data that the organisation holds, and you must implement reasonable and appropriate security measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage.

You must be particularly careful in protecting special category personal data and criminal records personal data.

You must follow all procedures - and comply with all technologies and safeguards - that the organisation put in place to maintain the security of personal data, from the point of collection to the point of destruction.

Where the organisation uses third-party service providers - to process personal data on the organisation's behalf - additional security arrangements need to be implemented in contracts with those third parties to safeguard the security of personal data. You can only share personal data with third-party service providers if you have been authorised to do so and provided that certain safeguards and contractual arrangements have been put in place, including that:

- The third party has a business need to know the personal data for the purposes of providing the contracted services
- Sharing the personal data complies with the privacy notice that has been provided to the data subject - and, if required, the data subject's consent has been obtained
- The third party has agreed to comply with the organisation's data security procedures and has put adequate measures in place in ensure the security of processing
- The third party only acts on the organisation's documented written instructions
- A written contract is in place between the organisation and the third party that contains specific approved terms
- The third party will assist the organisation in allowing data subjects to exercise their rights in relation to data protection and in meeting the organisation's obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments

- The third party will delete or return all personal data to the organisation at the end of the contract
- The third party will submit to audits.

Before any new agreement involving the processing of personal data by a third-party service provider is entered into, or an existing contract is amended, you must seek the approval of its terms from the person with responsibility for data protection, named at the beginning of this document.

You may only share personal data with other members of the organisation's staff if they have a business need to know in order to properly perform their job duties and responsibilities.

Hard copy personnel files, which hold personal data gathered during the working relationship, are confidential and must be stored in locked filing cabinets. Only authorised members of staff, who have a business need to know in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets or locked drawers and cupboards when not in use by authorised members of staff. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised members of staff have access to those data.

The organisation has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.

The data protection legislation requires the organisation to notify any personal data breach to the **Information Commission within 72 hours** after becoming aware of the breach and - where there is a high risk to the rights and freedoms of data subjects - to the data subject themselves.

A personal data breach is any breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and includes any act or omission that compromises the confidentiality, integrity or availability of personal data or the safeguards that the organisation - or the organisation's third-party service providers - have put in place to protect them.

The organisation has procedures in place to deal with any suspected personal data breach and you are required to comply with these.

If you know or suspect that a personal data breach has occurred, you must immediately contact the person with responsibility for data protection - named at the beginning of this document - retain any evidence you have in relation to the breach, and follow the organisation's Data Breach Policy and Response Plan.

Accountability

The organisation is responsible for - and must be able to demonstrate compliance with - the data protection principles. This means that the organisation must implement appropriate and effective technical and organisational measures to ensure compliance and you are also required to fully assist and co-operate with the organisation in this regard. In particular, the organisation have:

- Appointed a person - named at the beginning of this document - to be responsible for data protection compliance and privacy matters within the organisation
- Kept written records of personal data processing activities
- Implemented a **Privacy by Design** approach when processing personal data and the organisation will conduct and complete **Data Protection Impact Assessments** (**DPIAs**) where a type of data processing **e.g.** the launch of a new product or the adoption of a new program, process or IT system - in particular using a new technology - is likely to result in a high risk to the rights and freedoms of data subjects
- Integrated data protection requirements into the organisation's internal documents - including this **Data Protection Policy** - other related policies and privacy notices
- Introduced a regular training programme for all members of staff on the data protection legislation and on their data protection duties and responsibilities and the organisation also maintain a training record to monitor its delivery and completion - **you must undergo all mandatory data protection training**
- Introduced regular reviews of the organisation's privacy measures, as well as all policies, procedures and contracts - and regular testing of the organisation's systems and processes - to monitor and assess the organisation's ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

The organisation also keep records of its personal data processing activities and you are required to assist the organisation in ensuring these records are full, accurate and kept up to date.

Privacy by design and data protection impact assessments

The organisation are required to implement **Privacy by Design** measures when processing personal data by implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation. You must assess what **Privacy by Design** measures can be implemented on all processes or systems that process personal data - where this is part of your job duties or responsibilities - because those processes or systems are under your control.

Where a type of data processing - e.g. the launch of a new product or the adoption of a new program, process or IT system which is under your control, is likely to result in a high risk to the rights and freedoms of data subjects, you must assist the organisation in conducting and completing a DPIA. This includes, but is not limited to:

- Systematic and extensive automated processing and automated decision-making activities - including profiling - and on which decisions are based that have legal effects, or similar significant effects, on data subjects
- Large-scale processing of special category personal data or criminal records personal data
- Large-scale systematic monitoring of publicly accessible areas **e.g.** using CCTV.

Before any form of new technology, program, process or system is introduced, you must contact the person with responsibility for data protection - named at the beginning of this document - in order that a DPIA can be carried out.

A **DPIA** will comprise a review of the new technology, program, process or system and it must contain a description of the processing operations and the purposes, an assessment of the necessity and proportionality of the processing in relation to those purposes, an assessment of the risks to individuals and the measures in place to address or mitigate those risks and demonstrate compliance.

Automated processing and automated decision-making

Automated processing is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, and **automated decision-making** occurs when an **electronic system** uses an individual's personal data to make a decision **without human intervention**.

The organisation does not carry out any automated processing and does not take any decisions based solely on automated decision-making, including profiling.

Direct marketing

The organisation is subject to certain rules when marketing to its clients and customers. If you are involved in direct marketing to customers, you must comply with the organisation's guidelines on this. In particular, a data subject's prior consent is required for electronic direct marketing.

There is a limited exception for existing clients and customers which allows the organisation to send marketing texts and e-mails if the organisation have obtained their contact details in the course of a sale to that person, are marketing similar products or services to them and the organisation gave that person an opportunity to opt out of marketing when first collecting their details and in every subsequent message.

If a data subject objects to direct marketing, it is essential that this is actioned in a timely manner and their details should be suppressed as soon as possible. You can retain just enough information to ensure that marketing preferences are respected in the future.

Transferring personal data to third countries

The data protection legislation restricts transfers of personal data to **third countries** and **international organisations** in order to ensure that the level of data protection afforded to data subjects is maintained.

The organisation does not transfer personal data to third countries or international organisations and you must ensure that you comply with this rule.

Data subject rights to access personal data

Under the data protection legislation, data subjects have the right, on request, to obtain a copy of the personal data that the organisation holds about them by making a written Data Subject Access Request (DSAR). This allows the data subject to check that the organisation is lawfully processing their personal data. The data subject has the right to obtain:

1. **Confirmation as to whether or not their personal data are being processed.**

2. **Access to copies of their specified personal data.**

3. **Other additional information.**

The other additional information - which should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language - comprises:

- The purposes of the processing and the categories of personal data concerned
- The recipients - or categories of recipients - to whom the personal data have been or will be disclosed, in particular recipients in third countries and international organisations
- Where the personal data are transferred to third countries and international organisations, what appropriate safeguards are in place relating to the transfer
- The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the data subject's rights to request rectification or erasure of their personal data or restriction of processing of their personal data or to object to such processing
- Their right to lodge a complaint with the **Information Commission** if they think that the organisation has failed to comply with their data protection rights
- Where the personal data are not collected from them, any available information as to their source
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the envisaged consequences of such processing for them.

When a data subject makes a **DSAR**, the organisation will log the date on which the request was received and confirm their identity. Where the organisation have reasonable doubts concerning the data subject's identity, the organisation will request them to provide such additional information necessary to confirm their identity before complying with their **DSAR**. The organisation will then search databases, systems and other places where the personal data which are the subject of the **DSAR** may be held. Where the organisation process a large quantity of personal data about a data subject, the organisation may ask them to first specify the information that their **DSAR** relates to.

If the data subject makes their **DSAR** electronically, the organisation must provide a copy of the personal data in a commonly used electronic format, unless they specifically request otherwise. If the data subject wants additional copies of the personal data, the organisation will charge a reasonable fee - which is based on our administrative costs of providing the additional copies.

The organisation will normally respond to a **DSAR** and provide copies of the personal data **within one month** of the date of receipt of the request. This time limit is calculated from the day that the request is received - whether it is a working day or not - until the corresponding calendar date in the next month. If this is not possible - because the following month is shorter and there is no corresponding calendar date - the date for response is the last day of the following month. If the corresponding date falls on a weekend or public holiday, the organisation have until the next working day to respond. However, the organisation may extend this time limit for responding by a **further two months** if the request is complex or there are a number of requests made by the data subject. If the organisation intend to extend the time limit, the organisation will contact the data subject **within one month** of the **DSAR**'s receipt to inform them of the extension and to explain why it is necessary.

Before providing the personal data to the data subject making the **DSAR**, the organisation will review the personal data requested to see if they contain the personal data of other data subjects. If they do, the organisation may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data. The organisation will also check whether there are any statutory exemptions from disclosure that apply to the personal data that are the subject of the **DSAR**. If a statutory exemption applies to any of the personal data, those personal data may not be disclosed.

Whilst the organisation will normally provide a copy of the personal data in response to a **DSAR** free of charge, the organisation reserve the right to charge a reasonable fee, based on the administrative costs of providing the personal data, when a **DSAR** is **manifestly unfounded** or **manifestly excessive** - particularly if it repeats a **DSAR** to which the organisation have already responded. Alternatively, where a **DSAR** is **manifestly unfounded** or **manifestly excessive**, the organisation reserve the right to refuse to respond altogether.

Where the organisation refuse to act on a request in this way, the organisation will set out our written reasons why to the data subject **within one month** of receipt of their **DSAR**. The organisation will also inform them of their right to complain to the **Information Commission** or to seek a judicial remedy in the courts.

If you wish to exercise your data subject access rights, please complete the organisation's Data Subject Access Request Form, or put the request in an e-mail, and send it to the person with responsibility for data protection - named at the beginning of this document. You will be informed if the organisation need anything further to verify your identity.

If you receive a **DSAR** from another data subject, you must immediately forward it to the person with responsibility for data protection - named at the beginning of this document - and they will deal with responding to it.

Other data subject rights in relation to their personal data

Data subjects have a number of other rights in relation to their personal data. When the organisation process data subjects' personal data, the organisation will respect those rights. It is the organisation's policy to ensure that requests by data subjects to exercise their rights in respect of their personal data are handled in accordance with the data protection legislation.

Subject to certain conditions, and in certain circumstances, data subjects have the right to:

- **Be informed** | this is normally satisfied by issuing them with an appropriate privacy notice.
- **Request rectification of their personal data** | this enables them to have any inaccurate or incomplete personal data the organisation hold about them corrected or completed, including by their providing a supplementary statement.
- **Request the erasure of their personal data** | this enables them to ask the organisation to delete or remove their personal data where there's no compelling reason for their continued processing **e.g.** it's no longer necessary in relation to the purpose for which they were originally collected, or if there are no overriding legitimate grounds for the processing.
- **Restrict the processing of their personal data** | this enables them to ask the organisation to suspend the processing of their personal data **e.g.** if they contest the accuracy and so want the organisation to verify the accuracy or the processing is unlawful, but they don't want the personal data to be erased.
- **Object to the processing of their personal data** | this enables them to ask the organisation to stop processing their personal data - where the organisation are relying on the legitimate interests of the business as the lawful basis for processing - and there is something relating to their particular situation which makes them decide to object to processing on this ground.
- **Data portability** | this gives them the right to request the transfer of their personal data to another party, so that they can reuse them across different services for their own purposes.
- **Not be subject to automated decision-making, including profiling** | this gives them the right not to be subject to a decision based solely on the **automated processing** of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them.
- **Prevent direct marketing** | this enables them to prevent the organisation's use of their personal data for direct marketing purposes.
- **Be notified of a data breach** | which is likely to result in a high risk to their rights and freedoms.

If, as a data subject, you wish to exercise any of these rights, please contact the person with responsibility for data protection - named at the beginning of this document.

If a data subject invokes any of these rights, you must take steps to verify their identity, log the date on which the request was received and seek advice from the person with responsibility for data protection - named at the beginning of this document - if you need assistance in dealing with the matter. The following response procedures apply as applicable:

- **Response to requests to rectify personal data** | unless there is an applicable exemption, the organisation will rectify the personal data without undue delay and will also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed **e.g.** the organisation's third-party service providers, unless this is impossible or involves disproportionate effort.

- **Response to requests for the erasure of personal data** | the organisation will erase the personal data without undue delay provided one of the grounds set out in the data protection legislation applies and there is no applicable exemption - and, where the personal data are to be erased, a similar timetable and procedure to that applying to responding to **DSAR**'s will be followed. The organisation will also communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. Where the organisation have made the personal data public, the organisation will take reasonable steps to inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data.

- **Response to requests to restrict the processing of personal data** | where processing has been restricted in accordance with the grounds set out in the data protection legislation, the organisation will only process the personal data (excluding storing them) with the data subject's consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another person, or for reasons of important public interest. Prior to lifting the restriction, the organisation will inform the data subject that it is to be lifted. The organisation will also communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort.

- **Response to objections to the processing of personal data** | where such an objection is made in accordance with the data protection legislation and there is no applicable exemption, the organisation will no longer process the data subject's personal data unless the organisation can show compelling legitimate grounds for the processing which overrides the data subject's interests, rights and freedoms or the organisation are processing the personal data for the establishment, exercise or defence of legal claims. If a data subject objects to the processing of their personal data for direct marketing purposes, the organisation will stop processing the personal data for such purposes.

- **Response to requests for data portability** | unless there is an applicable exemption, the organisation will provide the personal data without undue delay if the lawful basis for the processing of the personal data is **consent** or **pursuant to a contract** and the processing of those data is carried out by automated means - and a similar timetable and procedure to that applying to responding to **DSAR**'s will be followed.

In the limited circumstances where the data subject has provided their consent to the processing of their personal data for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. This will not, however, affect the lawfulness of processing based on consent before its withdrawal.

If, as a data subject, you wish to withdraw your consent to the processing of your personal data for a specific purpose, please contact the person with responsibility for data protection - named at the beginning of this document. Once the organisation have received notification that you have withdrawn your consent, the organisation will no longer process your personal data for the purpose you originally agreed to, unless the organisation have another lawful basis for processing.

If a data subject invokes their right to withdraw their consent, seek advice from the person with responsibility for data protection - named at the beginning of this document - if you need assistance in dealing with the matter.

Data subjects also have the right to make a complaint to the Information Commission at any time.

Your obligations in relation to personal data

You must comply with this policy and the data protection principles at all times in your personal data processing activities where you are acting on behalf of the organisation in the proper performance of your job duties and responsibilities. The organisation rely on you to help the organisation meet its data protection obligations to data subjects.

Under the data protection legislation, you should also be aware that you are personally accountable for your actions and you can be held criminally liable. It is a criminal offence for you knowingly or recklessly to obtain or disclose personal data - or to procure their disclosure to a third party - without the consent of the organisation **e.g.** taking clients' or customers' contact details or other personal data without the organisation's consent on the termination of your employment, accessing another employee's personal data without authority, or otherwise misusing or stealing personal data held by the organisation.

It is also a criminal offence to knowingly or recklessly re-identify personal data that has been anonymised without the consent of the organisation - where the organisation de-identified the personal data - and it is a criminal offence to alter, block, erase, destroy or conceal personal data with the intention of preventing their disclosure to a data subject following a **DSAR**.

Where unlawful activity is suspected, the organisation will report the matter to the Information Commission for investigation into the alleged breach of the data protection legislation - and this may result in criminal proceedings being instigated against you. The organisation may also need to report the alleged breach to a regulatory body. This conduct would also amount to a gross misconduct offence under the organisation's Disciplinary Procedure and could lead to your summary dismissal. If you are not an employee, you may have your contract with the organisation terminated with immediate effect.

You must also comply with the following guidelines at all times:

- Only access personal data that you have authority to access and only for authorised purposes **e.g.** if you need them for the work you do for the organisation, and then only use the data for the specified lawful purpose for which they were obtained
- Only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally
- Do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the organisation's website or posted on the Internet in any form - unless the data subject has given their explicit consent to this
- Be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request
- Where the organisation provides you with code words or passwords to be used before releasing personal data, you must strictly follow the organisation's requirements in this regard
- Only transmit personal data between locations by e-mail if a secure network is in place **e.g.** encryption is used for e-mail
- If you receive a request for personal data about another member of staff or data subject, you should forward this to the person with responsibility for data protection - named at the beginning of this document
- Ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with the organisation's rules on computer access and secure file storage
- Do not access another member of staff's personal data **e.g.** their personnel records, without authority, as this will be treated as gross misconduct and it is a criminal offence
- Do not obtain or disclose personal data - or procure their disclosure to a third party - without authority or without the organisation's consent, as this will be treated as gross misconduct and it is a criminal offence
- Do not write down - in electronic or hard copy form - opinions or facts concerning a data subject, which it would be inappropriate to share with that data subject
- Do not remove personal data, or devices containing personal data, from the workplace - with the intention of processing them elsewhere - unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures **e.g.** such as password protection, encryption or pseudonymisation to secure the data and the device - and it has been authorised by your line manager
- Ensure that, when working on personal data as part of your job duties and responsibilities when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- Do not store personal data on local computer drives, your own personal computer or on other personal devices
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely **e.g.** by cross-shredding hard copies
- Ensure that you attend all mandatory data protection training
- Refer any questions that you may have about the data protection legislation or compliance with this policy to the person with responsibility for data protection - named at the beginning of this document.

Remember that compliance with the data protection legislation and the terms of this policy is your personal responsibility.

Changes to this policy

The organisation will review this policy at regular intervals and reserve the right to update or amend it at any time and from time to time. The organisation will circulate any modified policy to members of staff and, where appropriate, the organisation may notify you of changes by e-mail.

It is intended that this policy is fully compliant with the Data Protection Legislation. However, if any conflict arises between the Data Protection Legislation and this Policy, the organisation will comply with the Data Protection Legislation. This Policy may also be made available to the Information Commission.