

**Project Vision GDPR Data Protection 2018**

**Version 1.1**

**May 2018**

**Contents**

[1. Aims 3](#_Toc514941368)

[2. Legislation & Guidance 3](#_Toc514941369)

[3. Definitions 3](#_Toc514941370)

[4. The Data Controller 4](#_Toc514941371)

[5. Roles & Responsibilities 5](#_Toc514941372)

[6. Data Protection Principles 5](#_Toc514941373)

[7. Collecting Personal Data 6](#_Toc514941374)

[8. Sharing Personal Data 7](#_Toc514941375)

[9. Subject Access Requests and other Rights of Individuals 8](#_Toc514941376)

[10. Photographs & Videos 9](#_Toc514941377)

[11. Data Protection by Design & Default 9](#_Toc514941378)

[12. Data Security & Storage of Records 10](#_Toc514941379)

[13. Disposal of Records 10](#_Toc514941380)

[14. Personal Data Breaches 10](#_Toc514941381)

[15. Training 11](#_Toc514941382)

[16. Monitoring Arrangements 11](#_Toc514941383)

[Appendix 1 – Personal Data Breach Procedure 12](#_Toc514941384)

[**Appendix 2 - Privacy notice for staff** 14](#_Toc514941385)

# Aims

Project Vision (PV) aims to ensure that all personal data collected about customers, suppliers, staff, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

# Legislation & Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR and the ICO’s code of practice for subject access requests.

# Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Personal Data | Any information relating to an identified, or identifiable, individual.  This may include the individual’s:   * Name (including initials) * Identification number * Location data * Online identifier, such as a username   It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity. |

|  |  |
| --- | --- |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including information about an individual’s:   * Racial or ethnic origin * Political opinions * Religious or philosophical beliefs * Trade union membership * Genetics * Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes * Health – physical or mental * Sex life or sexual orientation |
| Processing | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.  Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data. |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

# The Data Controller

Project Vision processes personal data relating to customers, suppliers, staff, visitors and others, and therefore is a data controller.

Project Vision is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

# Roles & Responsibilities

This policy applies to **all staff** employed, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

**Board**

The board has overall responsibility for ensuring that Project Vision complies with all relevant data protection obligations.

**Data protection officer**

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data PV processes, and for the ICO.

Full details of the DPO’s responsibilities are set out in their job description.

Our DPO’s contact details are below:

Email: james.clark@project-vision.co.uk

Telephone: 01865 481484

**All staff**

Staff are responsible for:

* Collecting, storing and processing any personal data in accordance with this policy
* Informing PV of any changes to their personal data, such as a change of address
* Contacting the DPO in the following circumstances:
  + With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  + If they have any concerns that this policy is not being followed
  + If they are unsure whether or not they have a lawful basis to use personal data in a particular way
* If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
* If there has been a data breach
* Whenever they are engaging in a new activity that may affect the privacy rights of individuals
* If they need help with any contracts or sharing personal data with third parties

# Data Protection Principles

The GDPR is based on data protection principles that Project Vision must comply with.

The principles say that personal data must be:

* Processed lawfully, fairly and in a transparent manner
* Collected for specified, explicit and legitimate purposes
* Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
* Accurate and, where necessary, kept up to date
* Kept for no longer than is necessary for the purposes for which it is processed
* Processed in a way that ensures it is appropriately secure

This policy sets out how PV aims to comply with these principles.

# Collecting Personal Data

* 1. **Lawfulness, fairness and transparency**

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

* The data needs to be processed so that PV can **fulfil a contract** with the individual, or the individual has asked PV to take specific steps before entering into a contract
* The data needs to be processed so that PV can **comply with a legal obligation**
* The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone’s life
* The data needs to be processed so that PV, can perform a task **in the public interest.**
* The data needs to be processed for the **legitimate interests** of PV or a third party (provided the individual’s rights and freedoms are not overridden)
* The individual has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

* 1. **Limitation, minimisation and accuracy**

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

# Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

* Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  + Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  + Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  + Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

* The prevention or detection of crime and/or fraud
* The apprehension or prosecution of offenders
* The assessment or collection of tax owed to HMRC
* In connection with legal proceedings
* Where the disclosure is required to satisfy our safeguarding obligations
* Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our customers or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

# Subject Access Requests and other Rights of Individuals

1. **Subject access requests**

Individuals have a right to make a ‘subject access request’ to gain access to personal information that PV holds about them. This includes:

* Confirmation that their personal data is being processed
* Access to a copy of the data
* The purposes of the data processing
* The categories of personal data concerned
* Who the data has been, or will be, shared with
* How long the data will be stored for, or if this isn’t possible, the criteria used to determine this period
* The source of the data, if not the individual
* Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

* Name of individual
* Correspondence address
* Contact number and email address
* Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

1. **Responding to subject access requests**

When responding to requests, we:

* May ask the individual to provide 2 forms of identification
* May contact the individual via phone to confirm the request was made
* Will respond without delay and within 1 month of receipt of the request
* Will provide the information free of charge
* May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

1. **Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

* Withdraw their consent to processing at any time
* Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
* Prevent use of their personal data for direct marketing
* Challenge processing which has been justified on the basis of public interest
* Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
* Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
* Prevent processing that is likely to cause damage or distress
* Be notified of a data breach in certain circumstances
* Make a complaint to the ICO
* Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

# Photographs & Videos

As part of PV activities, we may take photographs and record images of individuals within Project Vision.

Uses may include:

* In brochures, newsletters, etc.
* Online on Project Vision website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

# Data Protection by Design & Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

* Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
* Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
* Completing privacy impact assessments where PV’s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
* Integrating data protection into internal documents including this policy, any related policies and privacy notices
* Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
* Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
* Maintaining records of our processing activities, including:
  + For the benefit of data subjects, making available the name and contact details of Project Vision and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  + For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

# Data Security & Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

* Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
* Papers containing confidential personal data must not be left on office desks, on tables, pinned to notice/display boards, or left anywhere else where there is general access
* Where personal information needs to be taken off site, staff must sign it in and out from the PV Oxford office
* Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
* Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored
* Staff who store personal information on their personal devices are expected to follow the same security procedures as for PV-owned equipment.
* Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

# Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on PV’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

# Personal Data Breaches

PV will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours.

# Training

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or PV’s processes make it necessary.

# Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect Project Vision’s practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the board.

# Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

* On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
* The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  + Lost
  + Stolen
  + Destroyed
  + Altered
  + Disclosed or made available where it should not have been
  + Made available to unauthorised people
* The DPO will alert the directors.
* The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
* The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
* The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people’s rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  + Loss of control over their data
  + Discrimination
  + Identify theft or fraud
  + Financial loss
  + Unauthorised reversal of pseudonymisation (for example, key-coding)
  + Damage to reputation
  + Loss of confidentiality
  + Any other significant economic or social disadvantage to the individual(s) concerned

If it’s likely that there will be a risk to people’s rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO on the Trust’s central systems.

* Where the ICO must be notified, the DPO will do this via the ‘report a breach’ page of the ICO website within 72 hours. As required, the DPO will set out:
  + A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  + The name and contact details of the DPO
  + A description of the likely consequences of the personal data breach
  + A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
* If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
* The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  + The name and contact details of the DPO
  + A description of the likely consequences of the personal data breach
  + A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
* The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
* The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  + Facts and cause
  + Effects
  + Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored by the DPO on the Trust’s central systems.

* The DPO and the Managing Director will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

**Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

**Appendix 2 - Privacy notice for staff**

Under data protection law, individuals have a right to be informed about how Project Vision uses any personal data that we hold about them. We comply with this right by providing ‘privacy notices’ (sometimes called ‘fair processing notices’) to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at Project Vision.

We, Project Vision, are the ‘data controller’ for the purposes of data protection law.

Our data protection officer is listed below (see ‘Contact us’ below).

**The personal data we hold**

We process data relating to those we employ, or otherwise engage, to work at Project Vision. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

* Contact details
* Date of birth, marital status and gender
* Next of kin and emergency contact numbers
* Salary, annual leave, pension and benefits information
* Bank account details, payroll records, National Insurance number and tax status information
* Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
* Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
* Performance information
* Outcomes of any disciplinary and/or grievance procedures
* Absence data
* Copy of driving licence
* Photographs
* CCTV footage
* Data about your use of PV’s information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

* Race, ethnicity, religious beliefs, sexual orientation and political opinions
* Trade union membership
* Health, including any medical conditions, and sickness records

**Why we use this data**

The purpose of processing this data is to help us run PV, including to:

* Enable you to be paid
* Facilitate safe recruitment.
* Support effective performance management
* Inform our recruitment and retention policies
* Allow better financial modelling and planning
* Enable ethnicity and disability monitoring
* Improve the management of workforce data across the sector

**Our lawful basis for using this data**

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

* Fulfil a contract we have entered into with you
* Comply with a legal obligation
* Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

* You have given us consent to use it in a certain way
* We need to protect your vital interests (or someone else’s interests)
* We have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify PV’s use of your data.

**Collecting this information**

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

**How we store this data**

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

**Data sharing**

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

* Financial organisations
* Central and local government
* Our auditors
* Survey and research organisations
* Trade unions and associations
* Health authorities
* Security organisations
* Health and social welfare organisations
* Professional advisers and consultants
* Charities and voluntary organisations
* Police forces, courts, tribunals
* Professional bodies
* Employment and recruitment agencies

**Transferring data internationally**

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

**Your rights**

1. **How to access personal information we hold about you**

Individuals have a right to make a **‘subject access request’** to gain access to personal information that PV holds about them.

If you make a subject access request, and if we do hold information about you, we will:

* Give you a description of it
* Tell you why we are holding and processing it, and how long we will keep it for
* Explain where we got it from, if not from you
* Tell you who it has been, or will be, shared with
* Let you know whether any automated decision-making is being applied to the data, and any consequences of this
* Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

1. **Your other rights regarding your data**

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

* Object to the use of your personal data if it would cause, or is causing, damage or distress
* Prevent your data being used to send direct marketing
* Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
* In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
* Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

**Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner’s Office:

* Report a concern online at <https://ico.org.uk/concerns/>
* Call 0303 123 1113
* Or write to: Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

**Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

Data Protection Officer: James Clark

Email: james.clark@project-vision.co.uk

Telephone: 01865 481484