**DATA PROTECTION POLICY**

**EFFECTIVE: DD/MM/YY**

**Important:** This is a generic template document. It requires

tailoring specifically for your organisation before being published. Professional advice should be taken before applying it.

**Should you require any further assistance then please contact the DPO Centre at** [www.dpocentre.com](http://www.dpocentre.com)**.**

Copyright©: The DPO Centre

# CONTENTS

[CONTENTS 2](#_Toc42073045)

[1 INTRODUCTION 3](#_Toc42073046)

[2 DEFINITIONS 3](#_Toc42073047)

[3 SCOPE 5](#_Toc42073048)

[4 PURPOSE 6](#_Toc42073049)

[5 OUR PROCEDURES 7](#_Toc42073050)

[6 SPECIAL CATEGORIES OF PERSONAL DATA 9](#_Toc42073051)

[7 RESPONSIBILITES 10](#_Toc42073052)

[8 RIGHTS OF INDIVIDUALS 13](#_Toc42073053)

[9 PRIVACY NOTICES (Optional section) 14](#_Toc42073054)

[10 DATA SUBJECT ACCESS REQUEST 16](#_Toc42073055)

[11 RIGHT TO ERASURE 17](#_Toc42073056)

[12 THIRD PARTIES 18](#_Toc42073057)

[13 AUDITS, MONITORING AND TRAINING 19](#_Toc42073058)

[14 REPORTING BREACHES 20](#_Toc42073059)

[15 COMPLIANCE 20](#_Toc42073060)

# INTRODUCTION

[Our organisation] is committed to protecting the rights and freedoms of data subjects (natural persons) and the safe and secure processing of their personal data in accordance with Data Protection Legislation.

Data Protection Legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003, all the foregoing as amended from time to time, and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our employees understand the rules governing their use of the personal data to which they have access during their work.

In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) (or Data Protection Manager if you are not obliged to appoint a DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

[Our organisation]’s leadership is fully committed to ensuring continued and effective implementation of this policy and expects all [Our organisation] employees share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy has been approved by [Our organisation]’s Chief Executive Officer, [Full Name].

# DEFINITIONS

|  |  |
| --- | --- |
| **Business purposes** | The purposes for which personal data may be used by us:  Personnel, administrative, financial, regulatory, payroll and business development purposes [add and delete as required].  *Business purposes include the following:*  *- Compliance with our legal, regulatory and corporate governance obligations and good practice*  *- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests*  *- Ensuring business policies are adhered to (such as policies covering email and internet use)*  *- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking*  *- Investigating complaints*  *- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments*  *- Monitoring staff conduct, disciplinary matters*  *- Marketing our business*  *- Improving services* |

|  |  |
| --- | --- |
| **Personal data** | ‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular 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 natural person.  *Personal data we gather may include: individuals' phone numbers, email addresses, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationalities, job titles, and CVs.* |
| **Special categories of personal data** | Special categories of personal data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.  *Special categories of personal data we may gather include: [complete as appropriate e.g. employee health data].* |

|  |  |
| --- | --- |
| **Data controller** | ‘Data controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law, the controller may be provided for in law. |
| **Data processor** | ‘Data processor’ means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller. |
| **Processing** | ‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| **Supervisory authority** | This is the national body responsible for data protection. The supervisory authority for our organisation is [the Information Commissioner’s Office]. |

# SCOPE

This policy applies to all processing of personal data whether:

* wholly or partly by automated means (i.e. by computer, apps or other digital system), or
* by other means (i.e. paper records) that form part of filing system or are intended to form part of a filing system.

This policy applies to all staff and anyone else working on our behalf including contractors, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies such as those relating to Internet and email use. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being implemented.

**Who is responsible for this policy?**

As our Data Protection officer (DPO), (or Data Protection Manager if you are not obliged to appoint a DPO) [name here] has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO/DPM for further information about this policy if necessary. [DPO/DPM contact details]

# PURPOSE

The purpose of this policy is to also provide guidance on the Data Protection Principles that apply when any personal data belonging to or provided by data subjects is collected, stored or transmitted.

It is therefore imperative that all employees, contractors and vendors, comply with the 6 Data Protection Principles, summarised below.

Personal data should:

1. Be processed fairly, lawfully and transparently
2. Be collected and processed only for specified, explicit and legitimate purposes
3. Be adequate, relevant and limited to what is necessary for the purposes for which it is processed
4. Be kept accurate and up to date. Any inaccurate data must be deleted or rectified without delay
5. Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed
6. Be processed in a manner that ensures security, using appropriate technical and organisational measures

**Accountability and transparency**

We must ensure accountability and transparency in all our use of personal data.

Data protection legislation obliges all employees to take a proactive approach to data protection.

In order to encourage best practice – and to avoid penalties from the Information Commissioner’s Office (ICO) (change if a different supervisory authority applies) – all employees are required to read this policy, to treat others’ personal data with due care and consideration and to ensure that the organisation is able to demonstrate compliance

# OUR PROCEDURES

Controlling vs. Processing data

[Our organisation] is classified as a data controller [and data processor]. We are a data controller of our employee HR data but also for the client/customer personal data we process as part of our Sales and Marketing functions. In doing so we must maintain our appropriate registration (i.e. our data processing fee) with the Information Commissioner’s Office (change if other supervisory authority applies).

[For Data Processors] [We are a data processor when [our organisation] is contracted by a third party organisation to offer a service to data subjects and process their personal data for the data controller. In doing so we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing without the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller.

As a data processor, we must:

* Not use a sub-processor without the written authorisation of the data controller
* Co-operate fully with the ICO or other supervisory authority
* Ensure the security of the personal data
* Keep accurate records of processing activities
* Notify the controller of any personal data breaches]

If you are in any doubt about how we handle data, contact the DPO/DPM for clarification.

**Lawful basis for processing data**

Where we are a data controller, we must process personal data lawfully in accordance with individuals’ rights under the first Principle. This means that we must establish a lawful basis for processing personal data.

Employees must therefore ensure that any personal data they are responsible for managing or working with has a written lawful basis approved by the DPO/DPM.

If we cannot apply a lawful basis, our processing does not conform to the first Principle and will be unlawful. Data subjects have the right to stop the processing of any personal data that has been unlawfully processed and have it erased.

At least one of the following bases must apply whenever we process personal data:

1. **Consent**  
   We hold recent, clear, explicit, and defined consent for the data subject’s data to be processed for a specific purpose.
2. **Contract**  
   Processing is necessary to fulfil a contract with the individual or because they have asked us to take steps prior to entering into a contract.
3. **Legal obligation**  
   Processing is necessary to meet a legal obligation (excluding a contract).
4. **Vital interests**  
   Processing is necessary to protect a person’s life.
5. **Public function**  
   Processing necessary to perform a task in the public interest or for an official function, and the task or function has a clear basis in law.
6. **Legitimate interest**  
   Processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual’s personal data which overrides the legitimate interest.

**Deciding which condition to rely on**

If you are assessing the lawful basis of processing, you must first establish that the processing is necessary to achieve your purpose. This means the processing must be a targeted, appropriate way of achieving a stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means that doesn’t require the use of the personal data. You must also only use the minimum data required to achieve the purpose (e.g. don’t use a full date of birth if an age or age range will do).

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

Consider the following factors and document your answers:

* What is the purpose for processing the data?
* Can it reasonably be done in a different way?
* Is there a choice as to whether or not to process the data?
* Who does the processing benefit?
* After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
* What is the impact of the processing on the individual?
* Are you in a position of power over them?
* Are they a vulnerable person?
* Would they be likely to object to the processing?
* Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions. All data processing must be reported to and recorded by the Data Protection Officer/DPM.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a Privacy Notice. This applies whether we have collected the data directly from the individual, or from another source. You must record how individuals are to be informed and for written communications keep a copy of the wording used. This must be reported to the DPO/DPM who will approve wording and include relevant information in [organisation’s] overall Privacy Notice published on our website.

If no other lawful basis applies, you may be able to rely on Legitimate Interests. If this is the case a Legitimate Interests Assessment (LIA) must be undertaken and documented. If you need to conduct an LIA, you must conduct the DPO/DPM who will assist in conducting and approving the assessment. Note that in most cases, Legitimate Interests is only likely to be a suitable legal basis where the processing has little likelihood of affecting the rights or freedoms of a data subject.

If you are responsible for assessing the lawful basis and implementing the Privacy Notice for a processing activity, you must have this approved by the DPO/DPM.

# SPECIAL CATEGORIES OF PERSONAL DATA

**What are special categories of personal data?**

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

* race
* ethnic origin
* political opinions including party support or membership
* religion
* philosophy
* trade union membership
* genetics
* biometrics (where used for ID purposes)
* health (mental and physical)
* sex life and sexual orientation

Whenever we process special category data, we must identify a condition for processing as well as a lawful basis. The condition for processing special categories of personal data must comply with the law. If we cannot identify a condition for processing special categories of data, that processing activity must cease.

[Our organisation] processes special categories of personal data so we can comply with legal obligations to ensure health and safety at work (change if required). For more information, please refer to our [DPO/DPM and HR Manager].

**Criminal record checks**

Any criminal record checks must be justified by law. Criminal record checks cannot be undertaken based solely on the consent of the data subject. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such. Please refer to our separate policy regarding Criminal Records Checks or processing data relating to criminal records [remove if not relevant].

# RESPONSIBILITES

**Our responsibilities**

* Analysing and documenting the type of personal data we hold
* Checking procedures to ensure they cover all the rights of the individual
* Identifying the lawful basis for processing data
* Ensuring consent procedures are lawful
* Implementing and reviewing procedures to detect, report and investigate personal data breaches
* Storing data in safe and secure ways
* Assessing the risk that could be posed to individual rights and freedoms should data be compromised

**Your responsibilities**

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

**Responsibilities of the Data Protection Officer/Manager**

* Keeping the board updated about data protection responsibilities, risks and issues
* Reviewing all data protection procedures and policies on a regular basis
* Arranging data protection training and advice for all staff members and those included in this policy
* Answering questions on data protection from staff, board members and other stakeholders
* Responding to individuals such as clients and employees who wish to know which data is being held on them by us
* Checking and approving with third parties that handle the company’s data any contracts or agreements regarding data processing
* Monitoring compliance with data protection legislation across the organisation

**Responsibilities of the IT Manager**

* Ensure all systems, services, software and equipment meet acceptable security standards
* Check and scan security hardware and software regularly to ensure it is functioning properly
* Research third-party services, such as cloud services the company is considering using to store or process data

**Responsibilities of the Marketing Manager**

* Approve data protection statements attached to emails and other marketing copy
* Assist the DPO/DPM to deal with data protection queries from clients, target audiences or media outlets
* Coordinate with the DPO/DPM to ensure all marketing initiatives adhere to data protection laws and the company’s Data Protection Policy

**Accuracy and relevance**

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

If you aren’t clear the purpose for which data was collected but wish to use it, or you wish to use it for another purpose, you must seek approval from the DPO/DPM who can confirm the purpose for which the data was collected and whether any proposed new purpose is compatible. Where the proposed use is significantly different, involves combining data from different sources, or otherwise might have a significant impact on data subjects, the DPO/DPM may require that a Data Protection Impact Assessment is undertaken.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO/DPM.

**Data security**

We must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO/DPM will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

**Storing data securely**

* In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
* Printed data should be shredded when it is no longer needed
* Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a [password manager](http://cybersecurityzen.com/cybersecurity/keep-data-safe-rise-password-managers-1654/) to create and store their passwords
* Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
* The DPO/DPM must approve any cloud used to store data
* Servers containing personal data must be kept in a secure location, away from general office space
* Data should be regularly backed up in line with the company’s backup procedures
* Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
* All servers containing sensitive data must be approved and protected by security software
* All possible technical measures must be put in place to keep data secure

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. If you are responsible for any data, you must consult with the DPO/DPM and ensure that an appropriate retention period is applied and the data included on the retention schedule. A copy of our Retention schedule can be obtained on request from the DPO/DPM.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without express permission from the DPO/DPM.

# RIGHTS OF INDIVIDUALS

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

## Right to be informed

* Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
* Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

## Right of access

* Enabling individuals to access their personal data and supplementary information.
* Allowing individuals to be aware of and verify the lawfulness of the processing activities being undertaken on their personal data.

## Right to rectification

* We must rectify or amend the personal data of an individual if requested because it is inaccurate or incomplete.

## Right to erasure

* We must delete or remove an individual’s data if requested and there is no compelling reason for its continued processing.

## Right to restrict processing

* We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
* We are permitted to store personal data if it has been restricted, but not process it further. We must retain just enough data to ensure the right to restriction is respected in the future.

## Right to data portability

* We must provide individuals with their data so that they can reuse it for their own purposes or across different services where we process it on the basis of consent or contractual obligation.
* We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

## Right to object

* We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task unless there is an overriding reason to continue the processing.
* We must respect the right of an individual to object to direct marketing, including profiling and will cease if an objection is received.
* We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

## Rights in relation to automated decision making and profiling

* We must respect the rights of individuals in relation to automated decision making and profiling.
* Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

We must deal with rights requests without undue delay and within one calendar month. However, we may extend the time to respond by a further two months if the request is complex or we have received a number of requests from the individual. We must let the individual know within one month of receiving their request and explain why the extension is necessary.

# PRIVACY NOTICES (Optional section)

**When to supply a privacy notice**

A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

**What to include in a privacy notice**

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

* Identification and contact information of the data controller and the data protection officer, if applicable
* The purpose of processing the data and the lawful basis for doing so
* The legitimate interests of the controller or third party, if applicable
* The right to withdraw consent at any time, if applicable
* The categories of personal data obtained (only for data not obtained directly from the data subject)
* Any recipient or categories of recipients of the personal data
* Detailed information of any transfers to third countries and safeguards in place
* The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
* The right to lodge a complaint with the [supervisory authority], and internal complaint procedures
* The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
* Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
* Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

At a minimum, all initial contacts with data subjects, or those which will require a new collection of or reason for processing data, must make reference to and link to the Privacy Notice on our website.

Where you are collecting new data or processing it in a new way you must seek advice from the DPO/DPM.

Where you cannot easily link to the Privacy Notice on the website when you are collecting data (for example for phone contacts) you must consult the DPO/DPM to agree how the Privacy Notice will be communicated.

# DATA SUBJECT ACCESS REQUESTS

**What is a data subject access request?**

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information, which means the information which should be provided in a privacy notice.

**How we deal with data subject access requests?**

* We must provide an individual with a copy of the information upon request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.
* If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the DPO/DPM before extending the deadline.
* We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO/DPM.
* Once a data subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

**Data portability requests**

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and you must receive express permission from the DPO/DPM first.

# RIGHT TO ERASURE

**What is the right to erasure?**

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

* Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
* Where consent is withdrawn
* Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
* The personal data was unlawfully processed or otherwise breached data protection laws
* To comply with a legal obligation
* The processing relates to a child

**How we deal with the right to erasure**

We can refuse to comply with an erasure request where processing is necessary for the following reasons:

* To exercise the right of freedom of expression and information
* To comply with a legal obligation for the performance of a public interest task or exercise of official authority
* For public health purposes in the public interest
* For archiving purposes in the public interest, scientific research, historical research or statistical purposes
* The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

**The right to object**

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

* We have legitimate grounds for processing which override the interests, rights and freedoms of the individual; or
* The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

**The right to restrict automated profiling or decision making**

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

* It is necessary for the entry into or performance of a contract.
* Based on the individual’s explicit consent.
* Otherwise authorised by law.

In these circumstances, we must:

* Give individuals detailed information about the automated processing.
* Offer simple ways for them to request human intervention or challenge any decision about them.
* Carry out regular checks and user testing to ensure our systems are working as intended.

# THIRD PARTIES

As a [data controller (and/or) data processor], we must have written contracts in place with any third party [data controllers (and/or) data processors] that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

[For controllers] As a data controller, we must only appoint processors who can provide sufficient guarantees under the [UK/EU] GDPR that the rights of data subjects will be respected and protected and the personal data will be kept secure.

[For processors] As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under the [UK/EU] GDPR and we will protect and respect the rights of data subjects.

**Contracts**

Our contracts must comply with the minimum contractual requirements set out in the [UK/EU] GDPR. Our contracts with [data controllers (and/or) data processors] must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our Data Processing Agreements with [data controllers (and/or) data processors] must include terms that specify:

* The processor will act only on the written instructions of the controller
* Those involved in processing the data are subject to a duty of confidence
* Appropriate measures will be taken to ensure the security of the processing
* Sub-processors will only be engaged with the prior consent of the controller and under a written contract
* The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under Data Protection Legislation
* The processor will assist the controller in meeting its Data Protection Legislation obligations in relation to the security of processing, notification of data breaches and performance of Data Protection Impact Assessments
* The processor will delete or return all personal data at the end of the contract
* The processor will submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations
* Nothing will be done by either the controller or processor to infringe Data Protection Legislation

If you are going to share data with another organisation, you must contact the DPO/DPM who can provide or advise on suitable wording. The agreement must be approved by the DPO/DPM.

# AUDITS, MONITORING AND TRAINING

## Data audits

Regular data audits to manage and mitigate risks will be carried out. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. You must conduct a regular data audit as required by the DPO/DPM and normal procedures.

## Monitoring

Everyone must observe this policy. The DPO/DPM has overall responsibility for this policy. [Our organisation] will keep this policy under review and amend or change it as required. You must notify the DPO/DPM of any breaches of this policy. You must comply with this policy fully and at all times.

## Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities change, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO/DPM.

# REPORTING BREACHES

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. For externally reportable breaches, [Our organisation] has a legal obligation to report the data breach to [name of supervisory authority] within 72 hours.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

* Investigate the failure and take remedial steps if necessary
* Maintain a register of compliance failures
* Notify the [name of supervisory authority] of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Data Breach Policy and Procedure for more details.

# COMPLIANCE

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer/Manager.

Any individual who considers that the Policy has not been followed in respect of Personal Data about themselves should also raise the matter with the Data Protection Officer/Manager.

Further information about the DPA 2018 and the UK GDPR can be found on the Information Commissioner’s Office (ICO) website: <https://ico.org.uk/>.