Data Protection Policy

Responsible officer	Louise Cartridge
Approved by	Susan Kirby
Approved date	5.5.23
Next review date	5.10.24

Version	Amendment	Pages	Date	Who
1	Policy Completed	20	01/05/18	EM
2	Policy checked and updated	20	18.04.2020	EM
3	Policy checked and updated	22	21.06.21	SK
4	Policy Reviewed	22	05.04.22	SK
5	Policy Reviewed	22	05.05.23	SK
6	Policy Reviewed	22	16.09.24	SK

I.INTRODUCTION

Castleview Group (CVG) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations. This policy sets out our accountabilities, obligations and approach to the use of personal data in our work.

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

This policy sets out how we seek to protect personal data and ensure that all staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data collection/processing activity is initiated to ensure that relevant compliance steps are addressed.

CVG is committed through its policy and procedures to ensure that it:

- Complies with the General Data Protection Regulations and good practice
- Protects the rights of staff, customers, suppliers and Directors
- Is open and honest about how stores, processes, uses and disposes of individual's data
- Provides training and support for staff who handle personal data so they can deal with it confidently and consistently
- Protects itself from the risks of a data breach or data theft

Applies to:

This policy applies to all staff of CVG Limited, who must be familiar with this policy, what it means in relation to their role, including their obligations and responsibilities under GDPR and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff and full training provided, before being adopted.

Context

Responsibilities:

DPO – Louise Cartridge

ICO – Number ZA126486

Our Data Protection Officer (DPO) has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy as necessary. Data Protection Officer Telephone Number: 0191 4922422. Email: info@castleviewgroup.co.uk

Aims of the Policy

- To ensure CVG meets the GDPR requirements for data processing, control, permission, sharing, access and retention.
- To ensure that all CVG staff understand their role within data protection and adhere to the requirements of GDPR within their role.

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *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 number, email address, home address, employer name and address, unique learner/staff/client number, educational background, financial and pay details (including bank details), details of certificates and other documentary evidence of qualifications, education and skills, marital status, gender, nationality, next of kin, job title, and CV.*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-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 gather may include: racial or ethnic origin, physical or mental health condition, and criminal offences (or related proceedings).*
Data controller	A controller determines the purposes and means of processing personal data. CVG Limited is a Data Controller, registered with the Information Commissioner's Office (ICO).

Data processor	A processor is responsible for processing personal data on behalf of a 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 Commissioners Office.

II.POLICY STATEMENT

The principles

CVG Limited shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation (GDPR). We will make every effort possible in everything we do to comply with these principles. The principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can and will only be collected for a specific purpose.

3. Data minimisation

Any data that we collect must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up-to-date.

5. Retention

We cannot store data longer than is necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show **how** we comply with each Principle. You are responsible for keeping a written record of how all the data processing activities you are responsible for comply with each of the Principles. This must be kept up to date and must be approved by our Data Protection Officer; the DPO is responsible for undertaking data flow pathway analysis and will undertake regularity audits in order to ensure that only agreed and permitted data is being processed and is following its approved pathway.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor the processing of their data
    - Creating and improving security and enhancing privacy procedures on an ongoing basis, through effective audit, improvement and impact assessment

III. CONTENT

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. processing data

CVG Limited is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

As a data processor, 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 to be out with 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 written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority

- Ensure the security of the processing
- 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, you must contact the DPO for clarification.

Lawful basis for processing data

We must establish a lawful basis for processing data. Ensure that any data you are responsible for managing has a written lawful basis approved by the DPO. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

4. **Vital interests**

Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**

The 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 making an assessment of the lawful basis, you must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. You cannot rely on a lawful basis if you can reasonably achieve the same purpose by some other means.

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

You must 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.

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 (see page 11)**. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

Special categories of personal data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of 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
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this **unless exceptional circumstances apply or we are required to do this by law** (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

Our responsibilities

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess 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

- Keeping the Directors updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Establishing our flows of data and undertaking audits to ensure that agreed data pathways are being complied with
- Arranging data protection training and advice for all staff members and those included in this policy. All staff will be provided with initial training upon the implementation of this policy and that training will include the testing of staff knowledge and understanding. New staff will be trained on the policy during their Induction of employment and all staff will have mandatory annual refresher training.
- Answering questions on data protection from staff, management, funders, prime contractors and other stakeholders
- Responding to individuals such as learners, 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 agreement regarding data processing

Responsibilities of the Operations Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Implementing the Data Security Policy in order to ensure that all reasonable measures are taken to ensure that personal information is kept safely and securely

Responsibilities of the Contracts Director

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO 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.

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

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO 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 our designated secure storage areas, where unauthorised personnel cannot access it
- Printed data must be shredded when it is no longer needed
- Data stored on a computer must be protected by strong passwords that are changed regularly. All staff laptops must be locked when not in use and no laptop must be left unattended in a public area. Passwords must never be disclosed to anyone else, including other staff members.
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used. They must not be placed in any postal service.
- The DPO must approve any cloud that may, in future, be used to store data
- Our servers, which contain personal data must be kept in a secure location, away from general office space and must be protected by security software
- Data must be regularly backed-up in line with our authorised backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- 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, as well as funder requirements for learning provision and legal requirements, but should be determined in a manner consistent with our Documents and Records Retention Policy.

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 company rules and procedures without express permission from the DPO.

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:

1. 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.

2. 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

3. Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay and no later than one month. This can be extended to two months with permission from the DPO.

4. Right to erasure

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

5. 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 enough data to ensure the right to restriction is respected in the future.

6. 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.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. 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.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. 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.

Privacy notices

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 mean 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.

We must provide individuals with information including: the purpose for processing their personal data, our retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.

We must provide privacy information to individuals at the time we collect their personal data from them.

We will regularly review, and where necessary, update privacy information. We will bring any new uses of an individual's personal data to their attention before we start the processing.

Getting the 'right to be informed' correct will support our compliance with other aspects of the GDPR and will build trust with people, but getting it wrong can leave us open to fines and lead to reputational damage.

We provide individuals with all the following privacy information:

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable).

- The contact details of our data protection officer (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

Subject Access Requests

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

An individual will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice

How we deal with subject access requests

We must provide an individual with a copy of the information they 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.

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 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.

Once a 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, without delay and no later than one month from the request. 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 first.

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

We can only refuse to comply with a right to erasure in the following circumstances:

- 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.
- 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.

Using third party controllers and processors

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

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

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

Contracts

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. 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 contracts must include terms that specify:

- Acting only on written instructions
- 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 GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract

- 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 on GDPR.

Criminal record checks

Any criminal record checks we undertake are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the 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. You must have approval from the DPO prior to carrying out a criminal record check.

Audits, Monitoring and Training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains 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. The DPO will establish and own the audit schedule, with findings reported directly to the Company Directors and resulting action plans approved by them and implemented by those confirmed accountable for each agreed action.

Monitoring

All staff must comply fully with this policy and at all times. The DPO has overall responsibility for this policy. CVG will keep this policy under review and amend or change it as required. You must notify the DPO of any breaches of this policy.

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, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

Training will be prior to implementation of this policy, or within the Induction process of your commencement of employment (whichever is the latter) and thereafter will consist of an annual refresher training activity. All training will include an assessment of knowledge and understanding. A combination of external and internal training will be used for efficiency and maximum responsiveness (eg to accommodate new employees on an ad-hoc basis).

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

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means that you must take action and report a breach as soon as you become aware of it. CVG has a legal obligation to report any data breaches to the relevant authority

and the timescale for this is set by the relevant authority (which will vary dependent upon the owner of the data concerned).

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

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the 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.

Notification to the DPO should be in writing, or where the disclosure is in person, a written account will be made and will be verified by the DPO and individual providing the information. It must be noted that all disclosure of breaches will be considered in confidence, in order that all staff feel confident in reporting them, without risk of their identity being disclosed to anyone that may have shown any incompetence, error, wilful non-compliant actions or neglect in their duties.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

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.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.