Policy title	Data Protection
Policy Owner / Data Protection Manager	Catherine Millan, CEO
Date approved	August 2026
Review date	August 2027

Data Protection Policy

1. Introduction

1.1 We promote a positive culture of data protection compliance across our business. We are committed to meeting our legal responsibilities and protecting the personal data of our clients, employees, workers, suppliers, training participants and other individuals we work with. Protecting the confidentiality, integrity and security of personal data is a responsibility we take seriously.

1.2 Be What You See Consultancy Ltd ("we" "us" "our") will normally act as the **Data Controller** for personal data relating to our employees and for personal data that we collect and use for our own business purposes.

1.3 In some circumstances, we may process personal data on behalf of a client or another organisation, for example when delivering commissioned training, consultancy, research or evaluation activities. In these circumstances, we may act as a **Data Processor** and will process personal data in accordance with the Data Controller's documented instructions and the requirements of UK data protection legislation.

1.4 This Policy applies to all personal data that we process, regardless of how or where that information is stored.

1.5 Personal data is any information relating to an identified or identifiable individual. This may include a person's name, contact details, identification number, location information, online identifiers or information about their actions or behaviour.

1.6 Because of the nature of our work, we may also process special category data. This can include information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification purposes, health, sex life or sexual orientation.

1.7 This policy also applies to personal data that has been pseudonymised where an individual could still be identified using additional information.

2. Data Protection Principles

2.1 We ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit, and legitimate purposes
- adequate, relevant and limited to what is necessary;
- accurate and where necessary, kept up to date;
- kept for no longer than is necessary;
- processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- transferred outside the UK only where appropriate safeguards are in place.

3. Lawful Basis for Processing

3.1 We will ensure that we have an appropriate lawful basis before collecting or processing Personal Data where we are acting as the Data Controller.

3.2 The lawful basis will depend on the purpose for which the information is being processed. We will identify and document the appropriate lawful basis and provide individuals with information about the purposes for which their Personal Data is used and the lawful basis we rely upon through our relevant privacy information.

3.3 Where we process special category Personal Data, we will identify both an appropriate lawful basis and an additional condition for processing special category data.

3.4 Where we act as a Data Processor on behalf of another organisation, the Data Controller is responsible for determining the purpose and lawful basis for the processing. We will process the information only in accordance with the Data Controller's documented instructions and our contractual obligations.

4. Data Subjects' Rights

4.1 Individuals have a number of rights in relation to their personal data. Depending on the circumstances, these include:

- **The right to be informed** – to receive clear information about how and why we use their personal data.
- **The right of access** – to request access to personal data we hold about them.
- **The right to rectification** – to ask us to correct inaccurate or incomplete personal data.
- **The right to erasure** – to ask us to delete personal data in certain circumstances.
- **The right to restrict processing** – to ask us to restrict how personal data is used in certain circumstances.
- **The right to data portability** – to receive certain personal data in a structured, commonly used and machine-readable format and, where applicable, have it transferred to another organisation.
- **The right to object** – to object to certain types of processing, including direct marketing.
- **Rights relating to automated decision-making and profiling** – including rights relating to decisions based solely on automated processing where these have legal or similarly significant effects.

We will respond appropriately to requests from individuals seeking to exercise their rights.

5. Privacy by Design and Data Protection Impact Assessment (DPIA)

5.1 We will consider data protection and privacy when developing new services, systems, projects or ways of working and will use appropriate technical and organisational measures to protect personal data.

5.2 Data Protection Impact Assessment (DPIA) will be undertaken where proposed processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA may also be

used where we believe it would be good practice to assess the privacy implications of a new project or significant change.

6. Record of Processing Activities

6.1 We will maintain appropriate records of our personal data processing activities. These may include:

- the purposes for which information is processed;
- the categories of individuals whose information we hold;
- the types of personal data processed;
- who information is shared with;
- applicable lawful bases;
- retention arrangements; and
- details of relevant international transfers.

The level of documentation we maintain will be proportionate to the nature, scale and risk of our processing activities.

7. Third Party Processing

7.1 Where we appoint a third party to process personal data on our behalf, we will take reasonable steps to ensure that the organisation provides appropriate data protection and security safeguards.

7.2 Appropriate contractual arrangements will be put in place where required, and our use of third-party processors will be kept under review.

8. Data Protection Responsibility

8.1 The Data Protection Manager (DPM) is responsible for overseeing this policy and our approach to data protection.

8.2 Questions about this policy, the use of Personal Data or an individual's data protection rights should be referred to the DPM.

8.3 Everyone working on behalf of Be What You See Consultancy Ltd who has access to Personal Data has a responsibility to handle it appropriately and in accordance with this policy.

9. Privacy notices

9.1 We will provide individuals with appropriate privacy information explaining how and why their personal data is collected and used. This may include privacy information for employees, clients, training participants, website users and other people whose personal data we process.

9.2 Privacy information will be written as clearly as possible and will be reviewed when our processing activities change.

10. Training and Awareness

10.1 Everyone who handles personal data on our behalf will be made aware of their responsibilities for protecting personal data and maintaining confidentiality.

10.2 Employees will be required to read and understand this policy as part of their induction. Appropriate information, guidance or training will be provided and refreshed where necessary.

11. Consent

11.1 Consent is one of the lawful bases that may be used for processing personal data. We will only rely on consent where it is appropriate to do so.

11.2 Where we rely on consent, it will be freely given, specific, informed and unambiguous, and we will maintain appropriate evidence that consent has been obtained.

11.3 Individuals will be able to withdraw their consent at any time. Withdrawing consent will not affect the lawfulness of processing carried out before consent was withdrawn.

12. Data Retention

12.1 We will retain personal data only for as long as necessary for the purpose for which it was collected, including where information needs to be retained to meet legal, contractual, accounting or reporting requirements.

12.2 When determining how long information should be retained, we will consider the nature and sensitivity of the information, why it is required, any risks associated with retaining it and any applicable legal or contractual requirements.

12.3 Personal data that is no longer required will be securely deleted, destroyed or anonymised as appropriate.

13. Safeguarding

13.1 Data Protection legislation does not prevent the appropriate sharing of information where this is necessary to safeguard a child or adult at risk. Concerns about data protection should not prevent appropriate information sharing where there is a genuine safeguarding concern.

13.2 Further information about our safeguarding procedures is contained in our relevant safeguarding policies and guidance.

14. Access to Personal Data

14.1 Individuals have the right to ask whether we process personal data about them and, subject to certain exemptions, to receive a copy of that information by making a Subject Access Request (SAR).

14.2 Requests should be forwarded to the Data Protection Manager, who will coordinate the response.

14.3 We will normally respond without undue delay and within one month of receiving the request. Where permitted by law, this period may be extended by up to a further two months where a request is complex or where a number of requests have been received.

14.4 We will not normally charge a fee for responding to a Subject Access Request. A reasonable fee may be charged, or a request refused, where permitted by law, including where a request is manifestly unfounded or excessive.

15. International transfer of personal data

15.1 Some of the third-party services we use may store or process personal data outside the United Kingdom.

15.2 Where personal data is transferred outside the UK, we will ensure that an appropriate mechanism or safeguard recognised under UK data protection legislation is in place where required. This may include UK adequacy regulations, the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses or another legally recognised mechanism.

15.3 We will maintain appropriate information about international transfers as part of our data protection records and will keep our third-party arrangements under review.

16. Information Security and Personal Data Breaches

16.1 We will take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful access, use, disclosure, alteration, loss, destruction or damage.

16.2 Anyone working on our behalf who becomes aware of an actual or suspected personal data breach must report it to the Data Protection Manager as soon as possible and preserve any relevant information or evidence.

16.3 We will investigate and record personal data breaches and assess the potential impact on the individuals affected.

16.4 Where a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the Information Commissioner's Office without undue delay and, where required, within 72 hours of becoming aware of the breach.

16.5 Where a breach is likely to result in a high risk to an individual's rights and freedoms, we will also inform the affected individual where required by law.

17. Changes to this Data Protection Policy

17.1 This policy will normally be reviewed annually and may be reviewed earlier where there is a significant change to legislation, regulatory guidance, our services or the way in which we process personal data.