Data Protection Policy

(Aligned with company document standards)

1. Introduction

This Policy sets out the obligations of ECS Consultants Limited, a company registered in England & Wales under number, **04556533,** whose registered office is at 148 Stockport Road, Cheadle, Manchester, SK8 2DP, ("the Company") regarding data protection and the rights of customers, business contacts, etc., ("data subjects") in respect of their personal data under the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018, and applicable updates introduced by the Data (Use and Access) Act 2025.

The UK GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must always be followed by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the UK GDPR. The UK GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be: -

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

2.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR to safeguard the rights and freedoms of the data subject.

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

3. The Rights of Data Subjects

The UK GDPR sets out the following rights applicable to data subjects: -

3.1 The right to be informed.
3.2 The right of access.
3.3 The right to rectification.
3.4 The right to erasure (also known as the 'right to be forgotten').
3.5 The right to restrict processing.
3.6 The right to object.
3.7 Rights with respect to automated decision-making and profiling.
3.8 The right to data portability.

4. Lawful, Fair, and Transparent Data Processing

The UK GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR states that processing of personal data shall be lawful if at least one of the following applies: -

4.1 The data subject has given consent to the processing of their personal data for one or more specific purposes.
4.2 The processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract with them.
4.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject.
4.4 The processing is necessary to protect the vital interests of the data subject or of another natural person.
4.5 The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
4.6 The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

The Company shall identify and document the lawful basis for each processing activity it undertakes and ensure that data subjects are informed of the applicable legal basis at the point of data collection.

Records of lawful bases shall be maintained as part of the Company's processing records.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes personal data as necessary for its business activities. This may include personal data collected directly from data subjects and, where applicable, from third parties.
5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in the Company Data Retention Policy (or for other purposes expressly permitted by the UK GDPR).
5.3 Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

6. Adequate, Relevant, and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

7. Accuracy of Data and Keeping Data Up to Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up to date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 The Company shall ensure that indicative retention periods or the criteria used to determine such periods are made available to data subjects.

9. Secure Processing

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

The Company shall implement appropriate access controls to ensure that personal data is accessible only to authorised personnel.

10. Accountability and Record-Keeping

The Company shall, where required, carry out Data Protection Impact Assessments (DPIAs) for processing activities that are likely to result in a high risk to individuals' rights and freedoms.

10.1 The Company has appointed a person responsible for data protection compliance (referred to in this Policy as the 'Data Protection Lead') acting as the Data Protection Officer where required under UK GDPR.

10.2 The Data Protection Lead shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the UK GDPR and other applicable data protection legislation.

10.3 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information: -

- 10.3.1 The name and details of the Company, its Data Protection Lead, and any applicable third-party data processors.
- 10.3.2 The purposes for which the Company collects, holds, and processes personal data.
- 10.3.3 Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates.
- 10.3.4 Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy); and
- 10.3.5 Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

This Policy shall be reviewed regularly and updated as necessary to reflect changes in law, guidance, or business practices.

11. Keeping Data Subjects Informed

11.1 The Company shall provide the information to every data subject: -

11.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

11.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its use: -

a) at the time of the first communication with the data subject, where the data is used to communicate with them; or

b) before any transfer of the personal data to another party; or

c) as soon as reasonably practicable and in any event within one month of obtaining the personal data.

11.2 The following information shall be provided: -

11.2.1 Details of the Company including, but not limited to, the identity and contact details of the Company's Data Protection Lead.

11.2.2 The purpose for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing.

11.2.3 Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data.

11.2.4 Details of the period for which personal data will be stored, or the criteria used to determine that period.

11.2.5 Details of the recipients or categories of recipients of personal data.

11.2.6 Details of the data subject's rights under the UK GDPR.

11.2.7 Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time.

11.2.8 Details of the data subject's right to lodge a complaint with the Information Commissioner's Office (https://ico.org.uk), the 'supervisory authority' under the UK GDPR.

11.2.9 Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

11.2.10 Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

11.2.11 Where applicable, details of any transfers of personal data outside the United Kingdom and the safeguards in place.

12. Data Subject Access

12.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

12.2 Data subjects wishing to make a subject access request should do so using a Subject Access Request Form, sending the form to the Company's Data Protection Lead at ecsadmin@ecs-ecs.co.uk.

12.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

12.4 All SARs received shall be handled by the Company's Data Protection Lead.

13. Rectification of Personal Data

13.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

13.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

13.3 If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

14. Erasure of Personal Data

14.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances: -

14.1.1 It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed.

14.1.2 The data subject wishes to withdraw their consent to the Company holding and processing their personal data.

14.1.3 The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so).

14.1.4 The personal data has been processed unlawfully.

14.1.5 The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

14.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 If any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

15. Restriction of Personal Data Processing

15.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

15.2 If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

16. Objections to Personal Data Processing

16.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling).

16.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

16.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

17. Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data: -

17.1 Emails containing personal data shall be protected using appropriate security measures, including encryption where necessary based on risk.

17.2 Emails containing personal data should be appropriately labelled where necessary to reflect their sensitivity.

17.3 Personal data must not be transmitted over networks unless appropriate security measures are in place.

17.4 Personal data contained in emails shall be retained only where necessary and managed in accordance with the Company's data retention and security policies.

17.5 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

18. Data Security – Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data: -

18.1 All electronic copies of personal data should be stored securely using passwords and data encryption.
18.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.
18.3 All personal data stored electronically should be backed up and stored securely using appropriate technical and organisational measures. All backups should be encrypted.
18.4 Personal data stored on mobile devices must be protected by appropriate technical and organisational security measures.
18.5 No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

19. Data Security – Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

20. Data Security - Use of Personal Data

Where the Company engages data processors, it shall ensure compliance with Article 28 UK GDPR through written agreements.

The Company shall ensure that the following measures are taken with respect to the use of personal data: -

20.1 Personal data shall not be shared informally. Any sharing of personal data must be authorised and carried out in accordance with this Policy.
20.2 Personal data shall only be transferred to employees, agents, contractors, or other parties where such transfer is necessary and authorised, and appropriate safeguards are in place.
20.3 Personal data must always be handled with care and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time.
20.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

21. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security: -

21.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. Passwords must be strong, unique, and in line with current security best practices.
21.2 Passwords must be kept secure and must not be shared. Secure password management practices must be followed.
21.3 All software (including, but not limited to, applications and operating systems) shall be kept up to date.
21.4 No software may be installed on any Company-owned computer or device without the prior approval of the Managing Director, Stephen Levell.

22. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data: -

22.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the UK GDPR and under this Policy, and shall be provided with a copy of this Policy.
22.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company.
22.3 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so.
22.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised.
22.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise.
22.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed.
22.7 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy.
22.8 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed.
22.9 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the UK GDPR and this Policy by contract.
22.10 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that all their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the UK GDPR; and
22.11 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

23. Complaints Handling

The Company shall maintain procedures to handle complaints from data subjects regarding the processing of their personal data and shall respond within a reasonable timeframe in accordance with applicable law.

24. Data Breach Notification

24.1 All personal data breaches must be reported immediately to the Company's Data Protection Lead.
24.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Lead must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
24.3 If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Lead must ensure that all affected data subjects are informed of the breach directly and without undue delay.

24.4 Data breach notifications shall include the following information: -

24.4.1 The categories and approximate number of data subjects concerned.

24.4.2 The categories and approximate number of personal data records concerned.

24.4.3 The name and contact details of the Company's Data Protection Lead (or other contact point where more information can be obtained).

24.4.4 The likely consequences of the breach.

24.4.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

25. International Transfers of Personal Data

The Company may transfer personal data outside the United Kingdom where necessary for its business operations.

Where such transfers occur, the Company shall ensure that appropriate safeguards are in place, including, but not limited to: -

- Transfers to countries deemed to provide an adequate level of protection by the UK Government; or
- The use of approved contractual mechanisms such as the UK International Data Transfer Agreement (IDTA).

Data subjects may request further information on the safeguards used by contacting the Company.