DATA PROTECTION POLICY

GDPR + BS ISO/IEC 27001:2022 + BS ISO/IEC 27002:2022

DATA
PROTECTION POLICY
GDPR +
BS ISO/IEC 27001:2022 +
ISO /IEC 27002:2022

This Data Protection Policy is the property of All Clear Services Limited (the Company) and must be returned upon request.

The Policy describes the personal data protection systems within the Company, and is intended to assist the recipient in understanding how the system works to maintain compliance with appropriate legislation.

The Systems outlined in the Policy are enforced by separate IMS Procedures which are considered confidential and may not be distributed outside the Company.

All Clear Services Limited
Chrysotile House
Unit 5, Heath Road
Darlaston
West Midlands
WS10 8LP
Telephone: 0121 526 4839
Facsimile: 0121 526 5234
e-mail: enquiries@allclearenv.com

Revision Status: *06*	**Date of Review:** *November 2024*	**Reviewed by:** *VWW*
Reason for Review *Annual Review* *Policy Statements as below – dates changed to denote review*		
Section	Brief details of revision	
1.1	*Data Protection Policy Statement date changed to denote review*	
1.2	*Data Protection Training Policy date changed to denote review*	

INDEX

1.1 DATA PROTECTION POLICY STATEMENT

The processing of personal data is essential to the delivery of our work activities; All Clear Services (the Company) are strongly committed to the rights of individuals whose data they collect and process and will comply with UK and EU laws related to personal information in- line with the EU General Data Protection Regulation (GDPR). and will ensure that such processing is carried out fairly, lawfully, and transparently.

Data protection legislation, and Article 8 of the European Convention on Human Rights recognise that there is a balance between the legitimate use of personal data by organisations to enable the effective and efficient delivery of services in the public interest and ensuring appropriate protection for the rights and freedoms of the individual(s) to whom the personal data relates.

The Company recognises the very considerable responsibilities it has to safeguard the personal information it holds about its employees and this comprehensive policy sets out how the Company will go about ensuring it meets its obligations.

To achieve this the Company have implemented a Data Protection process (DPP), embedded within our Integrated Management System, which is maintained and improved continuously.

The DPP ensures that the objectives of the Company and obligations under the law are met and ensures that controls are in place that reflect the level of risk that the Company is willing to accept and that enable the Company to meet all the regulatory, statutory and contractual obligations that are applicable.

Most importantly the DPP will enable the Company to protect the interests of individuals and all other relevant stakeholders.

To comply with the requirements of GDPR the Company will:

- Process personal information only where this is strictly necessary for legitimate organisational purposes
- Collect only the minimum personal information required for these purposes and not process excessive amounts of personal information
- Provide clear information to individuals about how their personal information will be used and who will be using the information
- Only process relevant and adequate personal information
- Process personal information fairly and lawfully
- Keep all personal information secure
- Maintain an inventory of the categories of personal information that is processed
- Ensure personal information is kept accurate and up to date
- Retain personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
- Respect individuals' rights in relation to their personal information as defined in the GDPR.
- Only apply exemptions permitted by data protection legislation;
- Develop and implement the DPP to enable the policy to be implemented
- Identify internal and external stakeholders and the degree to which these stakeholders are involved in the implementation and operation of the DPP
- Identify staff with specific responsibility and accountability for the ongoing maintenance and support of the DPP.

This Policy defines the levels of individual responsibility and arrangements throughout the Company; eventual responsibility for fulfilling the defined responsibilities and arrangements is vested in the undersigned,

Andy Astley
Managing Director
November 2024

1.2 DATA PROTECTION TRAINING POLICY

All Clear Services (the Company), induction programmes, line manager training and specific training and awareness programmes will be undertaken, either in-house or at external training providers, by staff and authorised Information and Communication Technology (ICT) users to enable them to be aware of their responsibilities towards data protection information security.

The Company will maintain and organise all training and records relating to GDPR within the Human Resources site on the company's management system; training will be relevant to each individual to ensure a full understanding of their roles and responsibilities.

The Company will ensure all staff are competent and kept updated on any GDPR and legislative changes and ensure that all staff understand their responsibility to ensure that personal information is protected and processed in accordance with Company procedures, considering any related security requirements.

The Company ensures that those with day-to-day responsibility for enabling the demonstration of compliance with the General Data Protection Regulation (GDPR) and good practice can demonstrate competence in their understanding of the GDPR and good practice, and how this should be implemented within the Company.

The Company will also ensure that these staff members remain informed about issues related to the management of personal information, where appropriate, by contact with external bodies. The Company will maintain a list of relevant external bodies, the most important of which is the Information Commissioner's Office.

The Data Protection Manager keeps records of the relevant training undertaken by each person who has this level of responsibility.

The Company will ensure that all staff understand their responsibility to ensure that personal information is protected and processed in accordance with Company procedures, considering any related security requirements.

All Company personnel will be given training to enable them to process personal information in accordance with Company procedures; this training will be relevant to the role that each employee performs within the Company.

The Data Protection Manager is responsible for organising relevant training for responsible individuals and staff generally, and for maintaining records of the attendance of staff at relevant training.

This Policy defines the levels of individual responsibility and arrangements throughout the Company; eventual responsibility for fulfilling the defined responsibilities and arrangements is vested in the undersigned,

Andy Astley
Managing Director
November 2024

2. SCOPE

This policy applies to the collection, use, sharing and other processing of all personal data held by the Company, in any format including paper, electronic, audio and visual. It applies to all employees, whether employed on a permanent, fixed term, or temporary (agency) basis.

3. GDPR DEFINITIONS AND LEGAL BASES FOR PROCESSING PERSONAL DATA

3.1 Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special category personal data	Personal data which is more sensitive in nature and which requires more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3.2 Legal bases for processing personal data

Term	Definition
Legal bases for processing <u>ordinary</u> personal data *[to be lawful, processing must fall within at least one of these legal bases]*	• Necessary for performance of legal obligation to which you are subject (**BUT** not a contractual obligation) • Necessary for the performance of the individual's employment contract or to take steps to enter into contract at individual's request (e.g. processing job applications) • Necessary for legitimate business interests – yours, or those of a third party to whom you disclose the personal data – **EXCEPT** where those interests are overridden by interests or fundamental rights and freedoms of individual • Individual has consented for specified purpose(s) **BUT** GDPR/ICO GUIDANCE SAY DO NOT USE IN THE EMPLOYMENT CONTEXT • Necessary to protect the vital interests of the individual or another person (generally only appropriate in exceptional 'life or death' situations)

Legal bases for processing special category personal data
*[to be lawful, processing must meet one of the legal bases from the **'ordinary'** list **and** one from the **'special category'** list]*

- Necessary to exercise/perform legal right/obligation connected with employment (**NOT** for contractual rights/obligations; and **NB** need to include additional information in the Employee Data Protection Policy)
- Necessary for purposes of establishing, exercising or defending legal claims
- Necessary for occupational medicine or assessing the working capacity of the employee
- Information has manifestly been made public by the individual
- Individual has given explicit consent for specified purpose(s) **BUT** GDPR/ICO GUIDANCE SAYS DO NOT USE IN THE EMPLOYMENT CONTEXT
- Necessary for reasons of substantial public interest, as defined in national law (this may permit equal opportunities monitoring)
- Necessary to protect individual's/someone else's vital interests and individual cannot consent (generally only appropriate in exceptional 'life or death' situations)

4. PERSONAL DATA PROCESSED BY THE COMPANY

The Company processes personal data relating to all employees in order to be able to carry out its core function of carrying out demolition, dismantling, asbestos removal, remediation and related activities; examples include:

- Application forms and CV's;
- Employee's name and address and next of kin contact details;
- Induction Training Records;
- Personal History/Training Record;
- Equal Opportunities in Employment Record;
- Details of employee's right to work in the United Kingdom;
- Contract of employment;
- Employee's training records, including photographic identities contained therein;
- Employee's medical records, including statutory medicals, fit to work medicals and any related information;
- Records of sickness absence and attendance;
- Financial records, including salaries, bonuses, etc.;
- Information attached to a reference number that could be used to identify an employee.

The Company determines the purposes and means of processing this personal data and so is a data controller.
The Company is registered as a data controller with the ICO and will renew this registration annually as required.
The Company will produce and maintain a record of its processing activities ('ROPA') and make this available to the Office of the Information Commissioner ('ICO') upon request. Appropriate information concerning the processing of personal data (e.g. why, how, for how long) in respect of which the Company is a data controller will be communicated by the Company to data subjects by means of appropriate privacy notices.

5. ROLES AND RESPONSIBILITIES

5.1 Data Protection Manager (DPM)

Article 37 of the GDPR identifies the appointment of a Data Protection Officer in three specific situations, if a public body, if the organisation's core activities require regular monitoring of personal data on a large scale or where the organisation's core activities require large scale processing of special categories of data.
The Company does not fall into any of these criteria; however, to ensure responsibility is clearly identified, to maintain consistency of approach and to provide a point of contact for matters relating to data protection, the Company have appointed a Data Protection Manager (DPM).
The Quality Manager will assume the responsibilities of the DPM and will be supported by the QHSE Manager and Managing Director.
The DPM is responsible for collecting, maintaining, storing and disposal of personal data in accordance with this policy; this may include any of the documentation detailed in *'Personal data processed by the Company'*; in addition, the DPM is responsible for any of the issues arising from staff queries previously described.

5.2 Company employees

Designated Managers and Supervisors are responsible for collecting personal data in accordance with this policy; this may include any of the documentation detailed in *'Personal data processed by the Company'* arising from new starters, appraisals and information received on Site for transmittal to the Office for retention or change of circumstance; this information will be kept secure and given to the DPM as soon as is practicable;
Individual members of staff have a duty to advise the DPM of any change(s) in their circumstances affecting data held by the Company; in addition, they can contact the DPM with regards to any personal data issues in the following circumstances:

- With any questions the Company is not immediately able to resolve about the operation of this policy and about GDPR/DPA 2018, for example in relation to the lawful use, secure handling, and retention of personal data;
- Where Data Protection rights have been exercised, e.g. subject access,right to erasure etc, and it is unclear what the Company needs to do to meet its obligations;
- If there has been a data breach;
- When engaging in a new activity that may affect the privacy rights of individuals and assistance is required to conduct a Data Protection Impact Assessment (DPIA);
- If assistance is required in order to ensure Data Protection requirements are met when carrying out procurement and contracting activity e.g. where another organisation may need to process personal data on behalf of the Company.

6. DATA PROTECTION PRINCIPLES

The Company will comply with the principles relating to the processing of personal data set out in the GDPR by putting in place processes to ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**'purpose limitation'**);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- Accurate and, where necessary, kept up to date (**'accuracy'**);
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (**'storage limitation'**);
- 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 (**'integrity and confidentiality'**).

The Company shall be responsible for, and be able to demonstrate compliance with, the above principles (**'accountability'**).

7. COLLECTING PERSONAL DATA

7.1. Lawfulness, fairness and transparency

The Company will only process personal data where it has met one of 6 'lawful bases' (legal reasons) to do so under Data Protection law:

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

For special categories of personal data, the Company also needs to meet one of the special category conditions for processing as set out in Article 9 of the GDPR (as supplemented by the DPA 2018); the conditions which the Company will mainly rely on are:

- Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law
- Processing is necessary for carrying out obligations under employment, social security or social protection law
- Processing is necessary to protect the vital interests of a data subject or another individual
- Explicit consent of the data subject

The Company is keenly aware of the additional protections set out in GDPR for personal data about employees and takes its responsibilities very seriously.

Privacy Notices

When collecting personal data from employees the Company will ensure that relevant information is provided setting out why/how the Company will be using the information, how long it will be kept for, and how individual rights can be exercised. The Company has produced a privacy notice for Company personnel; this will be issued to all Company personnel either upon joining the Company or as part of our GDPR implementation process.

7.2. Limitation, minimisation, accuracy and retention

Personal data will only be collected for specified, explicit and legitimate reasons and only to the extent that is necessary to carry out our works functions.

If personal data is to be used for reasons other than those given when it was first obtained, the Company will generally inform the individuals concerned before doing so and seek consent if it is necessary to do so; an

exception to this may be where it is necessary and imperative to share information where there are safeguarding concerns or in the event of an emergency, for example an accident at work.
The Company will ensure there are robust measures in place to ensure that the personal data it holds is accurate and kept up to date; this will include proactive actions in the form of quality checks of records, and appropriate remedial actions to amend/update records and in any case where the Company becomes aware of any inaccuracy in the personal data it holds.
The Company will retain personal data only for as long as is necessary in accordance with statutory and operational requirements. The Company has a comprehensive records management policy and retention schedule which sets out the length of time specific types of record need to be retained for embedded within our Integrated Management System and the actions the Company will take to ensure secure destruction/disposal.

8. SHARING PERSONAL DATA

There are situations where the Company may legitimately need to share information, for example, there is an issue with a member of staff that puts the safety of others at risk
The Company will share personal data with law enforcement and government bodies where legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes

The Company may also share personal data with emergency services and the local authority to help them to respond to an emergency situation that affects any of our employees.

9. DATA PROCESSORS

Suppliers/contractors may need to be provided with personal data in order to provide services to the Company or deliver services on behalf of the Company e.g. IT companies providing software platforms to the Company. When doing this, the Company will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law, in particular in relation to information security
- Ensure a data processor agreement is put in place between the Company and the contractor/supplier

10. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal data that the Company holds about them. This includes:

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

Subject access requests will usually be made in writing (e.g. by letter or email) but can also be made verbally. A request should include:

- Name of individual
- Correspondence address
- Details of the information requested

10.2 Employees access requests and response

When responding to requests, the Company:

- Will ask the individual to provide two forms of identification unless the Company is otherwise satisfied of the identity of the person making the request
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May extend the timescale for compliance by a further two months, where a request is complex or involves very large volumes of information; where this is the case the Company will inform the individual of this within one month, and explain why the extension is necessary

The Company will not disclose information if it:

- Might cause serious harm to the physical or mental health of the member of staff or another individual
- If the request is unfounded or excessive, the Company may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When the Company refuses a request, it will will tell the individual why, and tell them they have the right to complain to the ICO.

10.3 Other Data Protection rights of the individual

Individuals have a number of additional rights, including:

- The right to rectification i.e. to have inaccurate personal data rectified
- The right to erasure i.e. to have personal data erased – this is not an absolute right and only applies in certain circumstances
- The right to restriction – this means personal data can still be stored but not used. This is not an absolute right and only applies in certain circumstances
- The right to object to processing – a data controller can continue to process personal data if it can demonstrate it has compelling reasons to do so. Individuals have an absolute right to stop their personal data being used for direct marketing
- Rights in relation to automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

These rights can be exercised in writing or verbally. In most cases, the Company has one calendar month in which to respond.

11. BIOMETRIC RECOGNITION SYSTEMS

If and where the Company uses employees' biometric data as part of an automated biometric recognition system the Company will comply with the requirements of the Protection of Freedoms Act 2012.

Company personnel will be notified before any biometric recognition system is put in place or before they first take part in it; the Company will get written consent from at the employee before taking any biometric data and processing it.

Company personnel have the right to choose not to use the Company's biometric system(s). If a biometric system is introduced, alternative means of accessing the relevant services will be provided for those who do not wish to participate; in such cases the Company will ensure that any relevant data already captured is deleted.

As required by law, if an employee refuses to participate in, or continue to participate in, the processing of their biometric data, the Company will not process that data.

12. CLOSED CIRCUIT TELEVISION (CCTV)

The Company uses CCTV in various locations around the Company sites for the purposes of crime prevention, maintaining site security and for public safety. In doing so, the Company will follow ICO guidance along with other relevant industry codes of practice in relation to the use of CCTV.

Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

13. DATA PROTECTION BY DESIGN & DEFAULT

The Company's approach to compliance with data protection legislation will be underpinned by the principles of privacy by design and privacy by default.

'Privacy by design' means that the Company will take into account privacy issues from the very outset of planning for an activity that might involve the processing of personal data. When undertaking a new activity privacy considerations will be embedded throughout. Data Protection Impact Assessments will be carried out where required/deemed necessary

'Privacy by default' means that the Company will ensure that only personal data that is necessary for a specific purpose is processed.

The Company will not collect more personal data than is needed for the purposes concerned, process it in any ways other than than is necessary or store it longer than is needed.

14. DATA SECURITY & STORAGE OF RECORDS

The Company has appropriate physical, technical and organisational measures in place in order to ensure the security of personal data.

In particular:

- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Where personal information needs to be taken off site, this is kept to the minimum required and staff must sign it in and out from the Company office

- Strong Passwords that are at least 8 characters long containing a mixture of letters, numbers and special characters required to access Company computers, laptops and other electronic devices. Staff and employees are reminded to change their passwords at regular intervals
- Where the Company engages a data processor, due diligence is carried out to ensure stored securely and adequately protected

15. DISPOSAL OF RECORDS

This is covered in the Company's records management policy within the Integrated Management System (IMS) and the Employee Record of Processing.

16. PERSONAL DATA BREACHES

The Company has robust measures in place to protect the personal data it holds. However, in order to be prepared for any possible incident a data breach management policy has been produced. All Company personnel will be briefed on this. It is essential all staff understand that appropriate and necessary actions need to be taken quickly in order to remedy a breach and in order to ensure, in the event of a serious incident, the Company is in a position to notify the ICO within 72 hours.

17. TRAINING

The Company recognises that data protection training is crucial so that all Company personnel understand their responsibilities relating to Data Protection and the use of personal data.
Failure to comply with data protection legislation could lead to serious consequences, and in some cases may result in significant fines or criminal prosecution.
All Company personnel will be provided with data protection training as part of their induction process; the Company will also ensure attendance at training and awareness sessions to be provided to ensure this learning is cascaded within the Company.

18. MONITORING ARRANGEMENTS

The DPM, in association with the QHSE Director and QHSE Manager is responsible for monitoring and reviewing this policy. The policy will be reviewed annually and updated if necessary; the Company will ensure that all staff are aware of and have read this policy.

19. LINKS WITH OTHER POLICIES

This data protection policy is linked to other policies including
- Quality and Business Continuity Policy;
- Equal Opportunities and Diversity Policy;
- Fraud and Malpractice Policy;
- Bribery Policy.