FGP
CHARTERED SURVEYORS

Chartered Surveyors Specialising in Renewable Energy, Utilities and Infrastructure.



DATA PROTECTION POLICY

Version 7.0

fgplimited.co.uk

Regulated by RICS®

bmtrada UKAS MANAGEMENT SYSTEMS 0012

bmtrada UKAS MANAGEMENT SYSTEMS 0012

bmtrada UKAS MANAGEMENT SYSTEMS 0012

Achilles UVDB SILVER PLUS

Ref: FGP_Data Protection Policy_Version 7.0_18.12.25

Contents

1.	**Policy Statement**		**3**
2.	**Scope Data Protection**		**3**
3.	**What is Data Protection and GDPR**		**4**
4.	**Definitions**		**4**
5.	**Data Protection Act 2018 and UK GDPR**		**5**
6.	**Measure Adopted by FGP**		**7**
	6.1	Data Use	7
	6.2	Lawfulness, Fairness and Transparency	7
	6.3	Purpose Limitation	8
	6.4	Data Minimisation and Accuracy	9
	6.5	Data retention (Storage limitation)	9
	6.6	Integrity and Confidentiality (Security)	10
7.	**Data Subject Rights and Requests**		**11**
8.	**Breach Reporting**		**12**
9.	**Sharing and Transfers of Personal Information**		**13**
10.	**Responsibility for the Data Protection Policy**		**13**
11.	**Compliance with the Data Protection Policy**		**14**
12.	**Communication and awareness of this Policy**		**14**
13.	**Breaches of this Policy**		**14**

Appendix A - Personal information Retention Schedule 16
Appendix B - Data Protection - Do's and Dont's 17

Document Control

Issue Number	Replaces	Published	By	Details
V1.0		15.12.20	Fisher German Priestner Limited	Original
V2.0	V1.0	15.12.21	Fisher German Priestner Limited	Review of V1.0
V3.0	V2.0	15.12.21	Fisher German Priestner Limited	Review of V2.0
V4.0	V3.0	01.12.22	Fisher German Priestner Limited	Review of V3.0
V5.0	V4.0	18.12.23	FGP Surveyors Limited	Review of V4.0
V6.0	V5.0	18.12.24	FGP Surveyors Limited	Review of V5.0
V7.0	V6.0	18.12.25	FGP Surveyors Limited	Review of V6.0

1. Policy Statement

1.1. FGP Surveyors Limited ("FGP") is committed to conducting its' business with the highest standards of professionalism and integrity. One of our core values is Knowledge including full compliance with the Data Protection Act 2018, Data (Use and Access) Act 2025, the UK General Data Protection Regulation (UK GDPR) and The Privacy and Electronic Communications (EC Directive) Regulations 2003.

1.2. The purpose of this policy is to ensure FGP's compliance with all laws, rules and regulations governing Data Protection and Personal Information and to ensure that employees and third parties Personal Information is treated in an appropriate and lawful manner.

1.3. FGP recognises its' responsibility and is committed to managing the security of Personal Information of employees and third parties, including the collection, use, retention, transfer, disclosure and destruction of the same.

1.4. FGP are dedicated to compliance with data protection laws and principles and operate a Privacy by Design approach in being proactive rather than reactive, designing systems and processes to protect Personal Information and FGP have in place effective measures to minimise the risk of breaches and ensure that the Personal Information is protected.

1..5 This policy is to be read in accordance with the FGP's Data Breach Policy and Email, Internet and IT Policy.

1.6. This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Scope Data Protection

2.1. This policy applies to all individuals working at all levels of the organisation, including Directors, Associate Directors, Consultants and Employees including those who work part-time and fixed-term, casual and agency workers (collectively known as FGP Personnel and referred to as FGP Personnel in this policy).

2.2. We also expect individuals and organisations that we deal with, whether they be Clients, Suppliers, Subcontractors or other Stakeholders to act with the same high standards in relation to Data Protection and GDPR. Where relevant, we will include appropriate clauses in our contracts regarding data protection and GDPR and the consequences of data breaches. Evidence of such acts is likely to result in the termination of a contractual relationship with any such individual or organisation.

3. What is Data Protection and GDPR

3.1. The EU General Data Protection Regulation (EU) 2016/679 (GDPR) has been enacted in UK law though the Data Protection Act 2018 and Data (Use and Access) Act 2025 and subsequent amendments following the withdrawal of the UK from the European Union as part of the European Union (Withdrawal) Act 2018 and is now referred to as UK GDPR. UK GDPR governs the gathering and use of Personal Information in the UK.

3.2. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and subsequent amendments, governs how organisations undertake marketing, use cookies on websites and compile telephone directories.

4. Definitions

4.1. **Personal Information** is defined as "Any information relating to an identified or identifiable natural person; 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".

4.2. **Data Subject** is an identifiable living individual whom Personal Information is collected and processed.

4.3. **Data Audit** identifies the Personal Information held by FGP, the processing that occurs and the legal basis for processing.

4.4. **Processing** of Personal Information encompasses the entire lifetime of Personal Information in FGP's possession including the collection, management, use, retention and storage, transfer, disclosure and destruction of information.

4.5. **Processors** of Personal Information will only undertake the processing that a controller has requested for example storage on a cloud or email server.

4.6. **Controllers** of Personal Information make the decision on what Personal Information is gathered, who it is gathered on, the methods of gathering and subsequently what processing is to occur to the Personal Information.

4.7. **Information Commissioners Office (ICO)** is the UK's independent supervisory authority which upholds UK GDPR and PECR in the public interest.

5. Data Protection Act 2018 and UK GDPR

5.1. FGP is a Controller and Processor of Personal Information and we are legally obligated under UK GDPR to protect such information, and to process it (gather, use, store and destroy it) in compliance with and be able to demonstrate compliance with the UK GDPR and it's principles. In some instances FGP will be a Joint Controller with a Client however, this does not change the responsibilities of FGP.

5.2. The Data Protection Act 2018 and UK GDPR, sets out seven key data protection principles which govern the use of Personal Information as set out below.

Principle (a)- Lawfulness, fairness and transparency: All Personal Information must be processed lawfully, fairly and in a transparent manner. This means that Personal Information must be processed for one of the lawful bases of processing (lawfulness), that Data Subjects should be informed by FGP what processing will occur (transparency) and clearly explain what that processing is (fairness).

Principle (b)- Purpose limitation: All Personal Information must be collected for specified, explicit and legitimate purpose and no further or different processing must occur to that data that is incompatible with the original intended purpose.

Principle (c)- Data minimisation: All Personal Information must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that FGP must only obtain information which is required for the data processing and not obtain or store any Personal Information beyond what is strictly necessary.

Principle (d)- Accuracy: All Personal Information should be necessary, accurate and kept up to date. FGP has the responsibility and processes in place to ensure that all data is accurate and kept up to date and all old inaccurate data erased or rectified.

Principle (e)- Storage limitation: All Personal Information shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the Personal Information will be processed. This means that FGP must store Personal Information for as long as necessary and only for its intended purpose.

Principle (f)- Integrity and confidentiality (security): All Personal Information must be processed in a manner that ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This means that FGP must have appropriate organisational and technical measures in place to ensure the integrity and confidentiality of Personal Information is maintained at all times.

Principle (g)- Accountability: The Data Controller (FGP) shall be responsible for and be able to demonstrate compliance with the above principles.

5.3. Under Principle (a) of the Data Protection Act 2018 an organisation must meet one of the six lawful bases to process Personal Information and which are:

(a) **Consent:** the individual has given clear consent for you to process their Personal Information for a specific purpose.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital Interest:** the processing is necessary to protect someone's life.

(e) **Public Task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law

(f) **Legitimate Interest:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's Personal Information which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

5.4. **Special Category Data** – Within the GDPR and the Data Protection Act 2018 certain data is defined as being special category data. This is Personal Information which requires more protection due to its sensitivity. Special Category Data is defined as being on of the following categories of Personal Information:

- Personal Information revealing racial or ethnic origin;
- Personal Information revealing political opinions;
- Personal Information revealing religious or philosophical beliefs;
- Personal Information revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

5.5. FGP are aware that non-compliance with the Data Protection Act 2018, Data (Use and Access) Act 2025 and UK GDPR may result in complaints, warnings, reprimands, enforcement and penalty notices and in relation to data breaches possible fines of up to £17.5 Million or 4% of annual turnover, whichever is the higher.

6. Measures Adopted by FGP

6.1. Data Use

6.1.1. It is necessary for FGP to gather a certain amount of Personal Information about employees, clients, landowners, occupiers and affected third parties (Data Subjects). Data subjects have an expectation that their Personal Information is kept private, confidential, secure and used appropriately.

6.1.2. FGP undertake a Data Audit every year to identify the Personal Information held, the processing that occurs and the legal basis for processing and which is stored in a centralised location.

6.1.3. Where processing could result in a high risk to Data Subjects rights and freedoms, or if large amounts of Personal Information is to be processed (Personal Information on 10,000 Data Subjects), or if new technologies are being used to undertake processing then a Data Protection Impact Assessment (DIPA) must be undertaken to map out the data to be collected, the purpose, legal basis, risks and mitigation of those risks.

6.1.4. UK GDPR provides examples of processes situations where there is a high risk to Data Subjects such as systematic and extensive evaluation of Personal Information, automated processing and profiling and the processing on a large scale of special categories of data.

6.1.5. FGP do not undertake any of the processing which is provided in 6.1.2 and 6.1.3 however, if an instance arose FGP will undertake a DIPA based on the ICO's template prior to any information being processed.

6.1.6. FGP does not use or engage in profiling and automated decision making in the fulfilment of contracts and the administration of the business or personnel.

6.1.7. FGP does not send promotional or direct marketing material through digital channels such as mobile phones, email, internet or social media.

6.1.8. FGP do not undertake digital marketing other than in a "business to business" context when sending promotional material to potential clients. When sending digital marketing material FGP will have gain consent from the individual prior to sending the same.

6.2. Lawfulness, Fairness and Transparency

6.2.1. FGP obtain Personal Information by lawful and fair means and where appropriate with the knowledge and consent of the Data Subject concerned. Where a need exists to request and receive consent of a Data Subject prior to collection, use or disclosure of their Personal Information, FGP obtains that consent.

6.2.2. FGP gathers information from publicly available sources and not the Data Subject. When Personal Information is gathered from such a public source, FGP is exempt from providing the Data Subject with a Privacy Notice if FGP are confident that the Data Subject already has the information which FGP has obtained.

6.2.3. In practice FGP will meet with the Data Subject and confirm any Personal Information previously obtained and during this meeting the Privacy Notice will be provided or provided via FGP's website.

6.2.4. FGP process Personal Information fairly and in a manner that people would reasonably expect and does not process Personal Information in a manner that unjustifiably adversely affects the Data Subject.

6.2.5. FGP will, where it is considered it is reasonably appropriate, required by law or where required by contract, disclose to Data Subjects information as to the purpose of the processing of their Personal Information and what processing will be undertaken and this is referred to within this policy as a Privacy Notice. This will be provided when Personal Information is collected directly from the Data Subject unless a legal exemption applies to the requirements for disclosure and/or consent.

6.3. Purpose Limitation

6.3.1. FGP use Personal Information collected for the following broad purposes:

- The general running and business administration of FGP.
- To provide property consultancy services to FGP's clients and stakeholders with regard to a specific project for which the Personal Information will have been gathered.

6.3.2. If FGP are required to process Personal Information in a different way or for a new purpose than previously disclosed to the Data Subject, further consent will be sought from the Data Subject prior to this processing occurring.

6.3.4. FGP gathers and processes Personal Information from and about FGP Personnel to enable FGP to comply with legislation, to meet the needs of FGP's contract with FGP Personnel and to ensure the safety of FGP Personnel.

6.3.4. FGP only processes Special Category Data relating to FGP Personnel to meet FGP's obligations. All Special Category Data processed by FGP is subject to additional protection measures including password protected digital files and physical files stored in a separate secure location and which access is required by key.

6.3.5. FGP's website includes an online 'Privacy Notice' and online 'Cookie Notice' fulfilling the requirements of Data Protection Act 218, UK GDPR and Privacy and Electronic Communications Regulations 2003.

6.4. Data Minimisation and Accuracy

6.4.1. FGP ensures that all Personal Information it collects is complete and accurate and that such Personal Information is updated to reflect the current position of the Data Subject. The measures adopted by FGP to ensure data accuracy include:

- Correcting Personal Information known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject has not requested rectification of this data;
- Keeping Personal Information only for the period necessary;
- Removal of Personal Information in violation of any of the data protection principles or if the Personal Information is no longer required.

6.4.2. FGP ensure that all FGP Personal Information relating to FGP Personnel is reviewed and updated on an annual basis along with as and when informed of any changes by FGP Personnel to ensure that FGP's records are up to date and accurate.

6.5. Data Retention (Storage Limitation)

6.5.1 FGP only retain information for as long as it is required and annually review the information held to ascertain if retention of the Personal Information is necessary and delete all unnecessary information.

6.5.2. Following completion of a project FGP's files are archived and retained for up to 6 years to allow for any future claims that Data Subjects may have in relation to the 6 year limitation imposed by the Limitation Act 1980, to meet accounting best practices in relation to RICS compliant client accounts and to comply with Professional Indemnity Insurance requirements.

6.5.3. Personal Information of FGP Personnel will be retained during their employment at FGP and continuing afterwards to ensure that FGP meet the legal requirements including but not limited to, the Limitation Act 1980, Taxes Management Act 1970, Companies Act 2006, Statutory Sick Pay (General) Regulations 1982, The Statutory Maternity Pay Regulations 1986, Pensions Acts and The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995.

6.5.4. A Schedule of the retention periods have been provided in Appendix A.

6.5.5. FGP undertake a Data Audit annually to ensure that all Personal Information held has a purpose and is required to ensure that FGP meet the Data Retention and Minimisation requirements of UK GDPR, Data (Use and Access) Act 2025 and the Data Protection Act 2018.

6.6. Integrity and Confidentiality (Security)

6.6.1. FGP ensures that all Personal Information that is processed is secured by an appropriate technical and organisational measure against accidental loss, destruction or damage and against unlawful processing and detailed below.

6.6.2. All Personal Information is confidential and is not provided to anyone other than FGP's Clients (for whom the data is collected as Joint Controller) and co-consultant for the same or to meet FGP's legal obligations.

6.6.3. All digital information is stored only on an encrypted secure cloud server requiring an encryption key to access the server and can only be accessed from computers provided by FGP.

6.6.4. To prevent accidental data loss, the cloud server is backed up daily in its encrypted format to one of multiple locations provided by the cloud server provider and Personal Information is processed on behalf of FGP by the storage provider and could be stored in different locations around the UK. Alongside this, FGP operate two backup servers also backed up on a daily basis, one located at FGP's office and another secure offsite location to ensure against accidental loss, destruction or damage. Access to the backup servers is restricted to authorised FGP Personnel only.

6.6.5. FGP are provided a cloud based email services and all FGP Personnel are provided with email accounts and access to emails requires usernames and passwords. All Personal Information within email documentation is processed on behalf of FGP by the storage provider and could be stored in different locations around the UK.

6.6.6. Access to laptops, desktops and email accounts which are provided to FGP Personnel by FGP require usernames and passwords to access the same. All usernames and passwords are provided by FGP to FGP Personnel to ensure that the passwords are strong and with the use of upper and lower case characters and numbers.

6.6.7. No information is stored on any laptop or desktop computer provided by FGP and FGP do not permit the use of portable storage mediums such as hard drives or USB pen sticks.

6.6.8. All physical files are stored within FGP's office or in a secure offsite file storage facility when files have been archived and are processed on behalf of FGP by the storage provider and could be stored in different locations around the UK.

6.6.9. When physical files and documents are required to leave the office to fulfil the client's requirements, for exampled meetings, these files and documents are stored securely and in the possession of the FGP Personnel at all times.

6.6.10. All FGP Personnel files and Special Category Data, including the accident book, can only be accessed by authorised personnel and where appropriate, all digital files require passwords to open the same and physical files are stored in a separate locked and secure cabinet.

6.6.11. All paper waste from the office is shredded to ensure that any documents containing Personal Information can not be obtained by unauthorised individuals.

6.6.12. A Do's and Don'ts for Personal Information and procedures in FGP has been provided in Appendix B.

7. Data Subject Rights and Requests

7.1. The Data Protection Act 2018, Data (Use and Access) Act 2025 and UK GDPR ensures that Data Subjects have the following rights.

- The right to be informed – Data Subjects must be informed about the collection and use of their Personal Information.
- The right of access – Data Subjects have the right to request access to and copy of the Personal Information that is held by an organisation.
- The right to rectification – Data Subjects have the right to request inaccurate Personal Information to be rectified or completed if incomplete.
- The right to erasure (where applicable) – Data Subjects have the right to request Personal Information is erased if the data is no longer necessary for the purpose that it was collected, where consent is the legal basis and the consent is withdrawn, where Legitimate Interest is the legal basis and there is no legal basis for continued processing or there is a legal obligation to delete the data.
- The right to restrict processing – Data Subjects have the right to restrict the processing of Personal Information if accuracy is being contested, processing is unlawful, the information is no longer needed for the purpose of processing but it is required by the Data Subject for the establishment, exercise or defence of legal claims and if the data subject has objected to the processing, pending verification of that objection.
- The right to data portability- Data Subjects have the right to obtain and reuse their Personal Information for their own purposes and can only be exercised if automated processing is being carried out.
- The right to object - Data Subjects have the right to object to the processing of their Personal Information in certain circumstances
- Rights in relation to automated decision making and profiling – Data Subjects have the right to be informed about the automated processing and request human intervention.

7.2. Where a Data Subject wishes to submit a request under any of the above rights, this can be done verbally or in writing however, FGP will ask for all requests made verbally to also be confirmed in writing. Following receipt of this request it may be necessary for FGP to verify that it is the Data Subject submitting the request especially in relation to their right of access and portability to ensure that a data breach does not occur.

7.3. Where a request is submitted for access to or portability of a Data Subjects Personal Information, FGP will make reasonable efforts to find and retrieve the requested information and provide the same to the Data Subject in accordance with Section 7.6 below.

7.4. Where a request is submitted for the restriction of processing, FGP will ensure that the Personal Information is identified and access is restricted immediately to ensure that the Personal Information is stored only. Following this FGP will review the request, information, legal basis and processing involved and report to the Data Subject if FGP consider they have an overriding interest. If the information has been archived for storage purposes only then the Data Subject will be informed of the same.

7.5. Where a Data Subject requests erasure of information then FGP will review the situation, the data held and legal purpose and processing for the same and respond appropriately in accordance with Section 7.6 below. FGP however, have procedures in place to ensure that no Personal Information is retained longer than it is necessary to store and process that information.

7..6. All requests relating to a Data Subjects rights must be concluded within one month of receipt of the request. FGP will provide the information held in a suitable, accessible, concise and intelligible electronic format (unless the Data Subject requests otherwise) and in a secure format.

7.7. In certain circumstances, detailed in Schedules 2 and 3 of the Data Protection Act 2018, FGP can refuse a Data Subjects request under their rights, such as when information identifies other Data Subjects or information regarding negotiations with the Data Subject which FGP consider would prejudice those negotiations. If FGP refuse a request then the Data Subject must be informed of the reason why. Furthermore, the Data Subject has the right to make a complaint to the ICO or any other supervisory authority and the ability to seek enforcement of their right through the courts.

8. Breach Reporting

8.1. FGP have a Data Breach Policy which is to be followed at all times by FGP Personnel.

8.2. If a data breach occurs FGP's Data Protection Officer will undertake an investigation in accordance with FGP's Data Breach Policy.

9. Sharing of and Transfers of Personal Information

9.1. FGP does not share Personal Information with third parties other than the client whom all data is collected on behalf of, other consultants whom act on behalf of the client and statutory bodies to meet a legal requirement imposed on FGP or a client.

9.2. FGP shares Personal Information of FGP Personnel with UK government bodies such as HMRC to meet it's legal requirements. FGP will also share appropriate information to meet client requirements such as CV's and contact information.

9.3. UK GDPR, Data (Use and Access) Act 2025 and Data Protection Act 2018 prohibits the transfer of Personal Information outside of the UK unless that country has been deemed to have adequate data protection regimes in place. All countries within the European Economic Area (EEA) have been deemed as having adequate data protection regimes under UK GDPR.

9.4. FGP does not transfer information outside of the UK however, due to the nature of FGP's Clients and the companies that invest in UK infrastructure, a situation may arise where information would need to be transferred outside of the UK. If that transfer is to a country without adequate data protection regimes in place (ie. outside of the EEA) then FGP will only do so if adequate protections measures are in place such as using approved model contractual clauses and requiring companies in the USA to be signed up to certification such as Privacy Shield.

10. Responsibility for the Data Protection Policy

10.1. The FGP Board of Directors have overall responsibility for ensuring this policy complies with FGP's legal and ethical obligations and that all those under their control comply with it.

10.2. FGP have appointed Kieron Havard as the Data Protection Officer as it is important to have an individual responsible for data protection within the company. The Data Protection Officer has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it and updating internal control systems and procedures to ensure they are effective in protecting Personal Information.

10.3. Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it.

10.4. You are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries are encouraged and should be addressed to the FGP Data Protection Officer.

10.5. This policy and procedures are monitored annually and/or in accordance with any subsequent legislation or amendments to the Data Protection Act 2018, Data (Use and Access) Act 2025, UK GDPR and Privacy and Electronic Communications Regulations 2003 and amended as required with a new revision number. Any changes and updates are communicated to all FGP Personnel.

10.6. The top level management ie the Board of Directors are committed to ensuring that the privacy of those whom it collects Personal Information on and FGP Personnel, investigating data breaches and reporting the same where necessary to the ICO or other relevant enforcement agencies. The FGP culture promotes the importance of Data Subjects privacy and that a breach of the same is never acceptable.

11. Compliance with the Data Protection Policy

11.1. You must ensure that you read, understand and comply with this policy.

11.2. Protection of Personal Information in any part of our business or supply chains is the responsibility of all those working for FGP or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

11.3. You are encouraged to raise concerns about any issue in relation to the Data Protection Policy or suspicion that the Data Protection Policy is not being adhered to. If you believe or suspect a breach of this policy has occurred or that it may occur you must inform the FGP Data Protection Officer immediately.

11.4. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. We are committed to ensuring no one suffers any detrimental treatment as a result of reporting in good faith their suspicion that the protection of Personal Information is not being maintained and if a suspected data breach has occurred in whatever form in any part of our own business or in any of our supply chains.

12. Communication and awareness of this policy

12.1. Training on this policy and the protection of data within FGP forms part of the induction process for all individuals who work for us, and regular training will be provided.

12.2. Our commitment to the protection of Personal Information in our business and supply chains must be communicated to all suppliers, colleagues, contractors and business partners at the outset of our business relationship with them and reinforced as appropriate thereafter.

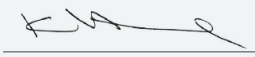
13. Breaches of this policy

13.1. Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

13.2. We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

Signed  Claire Priestner, Managing Director

Date 18.12.25

Signed  Kieron Havard, FGP Data Protection Officer

Date 18.12.25

APPENDIX A

Personal Information Retention Schedule

Personal Information Record Type	Contact details
Landowner, Occupier and Third Parties Personal Information in relation to Client Projects and Client Contact details	For the lifetime of project and up to 6 years following the completion of the project
Client Account Records	For the lifetime of project and up to 6 years following the completion of the project
Accident Book and Reports	3 Years
First Aid Training	6 Years
Fire Warden Training	6 Years
Payroll Records	6 Years or length of employment
HMRC, Income Tax and National Insurance Records	3 Years or length of employment
Maternity/Paternity Pay Records	3 years or length of employment
Pension Records	12 Years after benefit ceases
Personnel files	6 years from the termination of employment
Redundancy Details	6 years from the date of redundancy
Whistleblowing Documents	1 year or length of employment if substantiated investigation.
Working Time Records ie timesheets or annual holiday	6 years
CCTV Footage	1 month unless part of disciplinary procedure then 6 years from the termination of employment
CV's, Interview Notes and References	1 Year
Statutory Sick Pay Records	1 Year

APPENDIX B

Data Protection - Do's and Don'ts

Do:

- Only gather Personal Information that is required and relevant for the purpose.
- Seek advice from the Data Protection Officer if you are unsure if you can obtain Personal Information or if consent is required from the Data Subject.
- Seek consent when requesting information (if required) and provide FGP Privacy Notice when information is gathered.
- Update Personal Information if you know it to be incorrect.
- Review Personal Information held to ensure that it is up to date and correct.
- Treat Personal Information as if it was about you.
- Request a password is changed if you suspect that it may have been compromised and ensure all passwords are changed for work related accounts that use that password.
- Keep all software, operating systems and virus protection up to date on computers, laptops and mobile phones.
- Be vigilant when working away from office or in public places to ensure that third parties cannot obtain, overhear or view Personal Information.
- Report any lost or stolen equipment or documents immediately.

Don't:

- Obtain Personal Information that is not required or irrelevant for the purpose.
- Keep Personal Information if the purpose has been fulfilled and the information does not need to be retained.
- Give out Personal Information or provide access to documents containing any Personal Information other than to the Client or a Clients consultant.
- Change a password without consent and approval from management or use personal passwords for any work related account.
- Use Portable storage mediums such as hard drives, USB pen sticks or SD cards.
- Use any personal equipment to access and process company data.
- Leave computers unlocked or turned on when out of office.
- Leave hard copy documents unattended, unsecured or visible in cars when travelling and on site.
- Be scared to report anything to the Data Protection Officer if you have a concern.
- Deal with anything on your own, ensure that the Data Protection Officer and Directors are informed.
- Tell people or Data Subjects of a Data Breach of Personal Information or if you suspect a data Breach unless the Data Protection Officer has instructed you to do so.
- Publish any information relating to a project on social media including photographs.