St Francis Group Ltd

DATA PROTECTION POLICY

1. INTRODUCTION & SCOPE

1.1 The Company takes the security and privacy of data seriously. The Company needs to gather and use information or 'data' about employees, workers and consultants as part of their business and to manage these relationships.

1.2 The Company intends to comply with their legal obligations under the **Data Protection Act 2018** (the "2018 Act") and the **EU General Data Protection Regulation** ("GDPR") in respect of data privacy and security.

1.3 This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If a person falls within one of these categories, they are a "data subject" for the purposes of this policy.

1.4 The Data Protection Policy covers all information held in the Company's manual and computer files. The Company has measures in place to protect the security of this data.

1.5 The Company is a "data controller" for the purposes of your personal data. This means that the Company determines the purpose and means of the processing of your personal data.

1.6 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal date in the course of working for, or on behalf of, the Company.

1.7 The company is committed to being transparent about how it collects and uses personal data, and to meeting its data protection obligations.

1.8 The company has appointed Adrian Kennedy, Legal Director, St Francis Group Ltd, The Mill, One High Street, Henley in Arden, B95 5AA as Data Protection Officer/ Lead. Their role is to inform and advise the Company on its data protection obligations. They can be contacted at Adrian.Kennedy@stfrancisgroup.com or by writing to him as detailed above.

1.9 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

1.10 Definitions:

"Personal data" is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

2. DATA PROTECTION PRINCIPLES

2.1 Personal data must be processed in accordance with six Data Protection Principles. Personal data must:

- be processed fairly, lawfully, and in a transparent way;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate, and where necessary, kept up to date;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

The Company is accountable for these principles and must be able to show that they are compliant.

3. Defining personal data

3.1 "Personal data" means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into the Company's possession. It includes any expression of opinion about the person and an indication of the intentions of the Company or others, in respect of that person. It does not include anonymised data.

3.2 This personal data might be provided to the Company by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by the Company. It could be provided or created during the recruitment process or during the

course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.3 All correspondence and records pertaining to an individual employee's dealings within the Company in respect of their employment will be appended to the file mentioned above.

3.4 All personal data, whether it be stored electronically, on paper or on other materials, will be safely stored and treated as strictly confidential.

3.5 Personal files will be held in strict compliance with the GDPR.

3.6 The Company will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- any other category of personal data which we may notify you of from time to time.

4. Defining special categories of personal data

4.1 “Special categories of personal data” are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;

- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

The Company may hold and use any of these special categories of your personal data in accordance with the law.

5. Defining processing

5.1 "Processing" means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6. How the Company will process your personal data

6.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 The Company will use your personal data for one or more of the following purposes:

- performing the contract of employment (or services) between you and them e.g. administration of personnel, payroll and associated functions, processing data to the HMRC for tax purposes;

- complying with any legal obligation e.g. appropriate response to incidents, accidents and emergencies and the need to comply with HSE regulations; or

- if it is necessary for the Company's legitimate interests (or for the legitimate interests of someone else). However, the Company can only do this if your interests and rights do not override theirs. You have the right to challenge the Company's legitimate interests and request that they stop this processing. See details of your rights in section 13. below.

6.3 The Company can process your personal data for these purposes without your knowledge or consent. The Company will not use your personal data for an unrelated purpose without telling you about it and the legal basis that they intend to rely on for processing it.

6.4 If you choose not to provide the Company with certain personal data you should be aware that they may not be able to carry out certain parts of the contract between you both. For example, if you do not provide the Company with your bank account details, they may not be able to pay you. It might also stop the Company from complying with certain legal obligations and duties which they have, such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

6.5 The Company is registered with the Information Commissioner's Office and Adrian Kennedy is nominated as the Data Controller (DC).

6.6 The Company collects and processes personal information relating to members of staff, as a necessary part of complying with its obligations under the contract of employment and its legal requirements.

6.7 The Company will inform individuals of the purpose for which personal information is requested, processed, and the legal basis for processing in this policy and in its privacy notices. It will not process personal data of individuals for other reasons. Where the Company relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

6.8 Where the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with specific documented considerations on special categories of data and criminal records data.

6.9 The Company will update personal data promptly if an individual advises that their information has changed or is inaccurate.

6.10 Personal data gathered during employment is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Company holds HR-related personal data are outlined in the Data Retention & Disposal section of this policy below.

6.11 The Company keeps a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

7. Examples of when the Company might process your personal data

7.1 The Company has to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement). For example:

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with the Company;
- to check you have the legal right to work for the Company;
- to carry out the contract between you and the Company including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether the Company needs to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between you and the Company*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you and others with the Company's policies and contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect the Company *;

- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running the Company's business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- to seek legal advice from the Company's external consultants or legal advisers in connection with guidance around employment and HR issues*; and
- for any other reason which the Company may notify you of from time to time.

7.3 The Company will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, the Company can do so if they have your explicit consent. If the Company asked for your consent to process a special category of personal data then they would explain the reasons for the Company's request. You do not need to consent and can withdraw consent later if you choose by contacting Adrian Kennedy.

7.4 The Company does not need your consent to process special categories of your personal data when they are processing it for the following purposes, which they may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.5 The Company might process special categories of your personal data for the purposes above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with the Company's legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with the Company's legal obligations in respect of trade union members.

Performance-related Data

7.6 Review or appraisal is likely to involve the collection and recording of personal information. Information recorded should be relevant and should not be misleading. Managers carrying out appraisals must ensure that the record identifies the source of any comments, that opinions are not presented as facts, that information recorded is correct and not misleading and that if the employee has challenged the accuracy this is recorded and taken into account if / when the record is used for future employment decisions.

7.7 The employee must be provided with a copy of the completed appraisal form and should sign their agreement to the appraisal.

Disciplinary Data

7.8 Where a disciplinary warning has been issued to an employee, it will be kept on file and expunged when that expiry date has been reached. The information relating to the disciplinary matter may be retained in case it is required in future disciplinary proceedings but the warning itself will be deleted.

Medical Data

7.9 The Company operates policies and procedures that require information on an individual's medical status to be revealed to certain other employees of the Company e.g. the employee's manager, for example, please also see the Company Drug and Alcohol Policy and the Sickness and Absence Control Procedures. This information will be collected and processed in line with the company's position on special category data. Compliance with GDPR has been incorporated into these Policies.

7.10 In seeking Medical reports under the Access to Medical Records Act 1990, The Company will provide information to health professionals on a strict 'need to know' basis and employees will be fully informed of this information.

7.11 Medical testing of potential employees will only be requested by the Company if the individual is considered suitable for employment on all other grounds and only if it is a necessary and proportionate measure to: -

- determine the employee's fitness for continued employment;
- determine the employee's entitlement to health-related benefits e.g. sick pay;
- determine whether the potential employee is fit for the particular employment or
- meet any legal requirements for testing; or
- determine whether the potential employee is eligible to join a pension or insurance scheme.

8 Sharing your personal data

8.1 Sometimes the Company might share your personal data with group companies or the Company's contractors and agents to carry out the Company's obligations under their contract with you or for their legitimate interests. These will include seeking advice around employment law, health and safety, pensions etc.

8.2 The Company requires those companies to keep your personal data confidential and secure and to protect it in accordance with the law and their policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with the Company's instructions.

8.3 The Company does not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

9 How should you process personal data for the Company?

9.1 Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

9.2 The Company's Data Protection Officer is responsible for reviewing this policy and updating the Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

9.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

9.4 You should not share personal data informally.

9.5 You should keep personal data secure and not share it with unauthorised people.

9.6 You should regularly review and update personal data which you have to deal with for work. This includes telling the Company if your own contact details change.

9.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

9.8 You should use strong passwords.

9.9 You should lock your computer screens when not at your desk.

9.10 Personal data should be encrypted before being transferred electronically to authorised external contacts.

9.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

9.12 Do not save personal data to your own personal computers or other devices.

9.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.

9.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

9.15 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.

9.16 Personal data should be shredded and disposed of securely when you have finished with it.

9.17 You should ask for help from our Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security the Company can improve upon.

9.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with the Company's disciplinary procedure.

9.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

10 Data breaches

10.1 If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

10.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

11 International data transfers

11.1 We do not envisage transfer of personal data outside the EEA.

12 Subject access requests

12.1 Individuals have the right to make a subject access request. If an individual makes a subject access request, the company will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the Company has failed to comply with their data protection rights; and
- whether or not the Company carries out automated decision-making and the logic involved in any such decision-making.

12.2 The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

12.3 If the individual wants additional copies, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

12.4 To make a subject access request, the individual should send the request to the Data Controller, Adrian Kennedy. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify their identity and the documents it requires.

12.5 The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is excessive, numerous or the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell them if this is the case.

12.6 If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats

a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify them that this is the case and whether or not it will respond to it.

12.7 It is a criminal offence to conceal or destroy personal data which is part of a subject access request. This conduct would also amount to gross misconduct under the Company's disciplinary procedure, which could result in dismissal.

13 Your data subject rights

13.1 You have the right to information about what personal data the Company processes, how and on what basis as set out in this policy.

13.2 You have the right to access your own personal data by way of a subject access request (see above).

13.3 You can correct any inaccuracies in your personal data. To do you should contact HR/Emma Bromley or Accountant/Ann Chance.

13.4 You have the right to request that the Company erases your personal data where the Company were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact HR/Emma Bromley or Accountant/Ann Chance.

13.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact HR/Emma Bromley or Accountant/Ann Chance.

13.6 You have the right to object to data processing where the Company is relying on a legitimate interest to do so and you think that your rights and interests outweigh those of the Company and you wish the Company to stop.

13.7 You have the right to object if the Company processes your personal data for the purposes of direct marketing.

13.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. The Company will not charge for this and will in most cases aim to do this within one month.

13.9 With some exceptions, you have the right not to be subjected to automated decision-making.

13.10 You have the right to be notified of a data security breach concerning your personal data.

13.11 In most situations the Company will not rely on your consent as a lawful ground to process your data. If they do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact HR/Emma Bromley or Accountant/Ann Chance.

13.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and the Company's obligations.

14 Individual responsibilities

14.1 Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided changes, for example if an individual moves house or changes their bank details.

14.2 Individuals may have access to the personal data of other individuals in the course of their employment. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff.

14.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

14.4 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches

of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

15 Training

15.1 The Company will provide training to all individuals about their data protection responsibilities as part of the induction process.

15.2 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

16 Confidentiality

16.1 Any information received which is marked “private and confidential” should be opened by the addressee only or a member of the Management Team. Information received from any source in respect of an individual’s personal circumstances should be treated as confidential.

16.2 It is the responsibility of all staff to recognise the importance of the confidential nature of information held by the Company on its employees, and other personnel.

16.3 No member of staff should knowingly divulge confidential information to third parties about the individual circumstances of other employees, unless it conforms to the requirements of this policy.

16.4 It is the responsibility of all staff to ensure the security of confidential information in their keeping. Staff and client files should be locked away when not being used and particularly overnight. Staff should not leave confidential information in cars.

17 Monitoring

17.1 Monitoring of special category data including ethnic origin, sex or disability is an accepted employment practice provided it is used to promote equality of opportunity. The Company will ensure that the use of personal information about employees or applicants be kept to a minimum and this will only be collected anonymously if it is a legal obligation; a necessary element of an established programme for the promotion of equality of opportunity or it is otherwise needed because of some special feature of a particular job.

17.2 Information where used for equal opportunities monitoring will be kept in an anonymous format so that it cannot be linked to particular employees.

17.3 The Company reserves the right to introduce employee performance/ conduct monitoring schemes in those areas where it is actually necessary and proportionate to achieving the business purpose. All who are subject to the monitoring will be made aware that it is taking place, and the purpose for which information is collected unless in exceptional circumstances i.e. the monitoring is behavioural; and it is carried out for the purpose of preventing or detecting crime or the apprehension or prosecution of offenders; and informing employees would be likely to prejudice this purpose.

17.4 Information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced and employees were told about unless the information is such that no reasonable employer could ignore it i.e. it reveals criminal activity or gross misconduct. Employees will be presented with the information and given an opportunity to challenge or explain it before it is used.

18 FURTHER INFORMATION

18.1 This policy does not form part of your contract of employment and can be amended by the Company at any time.

18.2 Personal data should be shredded and disposed of securely when you have finished with it.

18.3 You should ask for help from the Company Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security they can improve upon.

18.4 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

18.5 If you have any concerns about how your data is processed in the first instance it is expected you will raise this with the Data Protection Officer. If however, you feel you have exhausted internal procedures and remain dissatisfied you have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.