Agricultural & Estate Services Limited – Data Protection Policy and Privacy Notice for Employees, Workers and Contractors

1. PURPOSE OF THIS DOCUMENT

1.1 The purpose of this document is to outline:

(a) How Agricultural & Estate Services Limited (**AES, we, us, our**) will ensure compliance with the UK GDPR and Data Protection Act 2018;

(b) Your responsibilities relevant to internal compliance;

(c) What information we collect about employees, workers and contractors and what we use it for.

1.2 This Data Protection Policy applies to all the Processing of Personal Data carried out by AES including processing carried out on its behalf by employees, agents, workers and contractors and by joint controllers, contractors and processors.

1.3 This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users, or any other Data Subject.

1.4 This Data Protection Policy applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Data Protection Policy when Processing Personal Data on our behalf and attend training on its requirements where we require you to do so.

Data protection is the responsibility of everyone within the Company and this Data Protection Policy sets out what we expect from you when handling Personal Data to enable the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

1.5 This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

1.6 This Data Protection Policy provides a framework for ensuring that AES meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

2. INFORMATION COVERED BY DATA PROTECTION LEGISLATION

2.1 The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

2.2 Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

2.3 Some personal data is more sensitive and is afforded more protection, this is information related to: Race or ethnic origin; Political opinions; Religious or philosophical beliefs; Trade

union membership; Genetic data; Biometric ID data; Health data; Sexual life and/or sexual orientation; and Criminal data (convections and offences). We do not and you should not collect any of this data. If you do inadvertently collect such data, please notify the DPO.

3. OUR COMMITMENT TO MEET DATA PROTECTION PRINCIPLES

3.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);

(b) collected only for specified, explicit and legitimate purposes (purpose limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);

(d) accurate and where necessary kept up to date (accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);

(g) not transferred to another country without appropriate safeguards in place (transfer limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

4. SCOPE OF POLICY AND WHEN TO SEEK ADVICE ON DATA PROTECTION COMPLIANCE

4.1 Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) You intend to do anything with Personal Data which is not already permitted by a Privacy Notice;

(b) if there has been a Personal Data Breach (paragraph 13);

(c) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);

(d) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 18) or plan to use Personal Data for purposes other than for which it was collected (see paragraph 8);

(e) if you plan to undertake any activities involving Automated Processing including profiling;

(f) if you need help complying with applicable law when carrying out direct marketing activities (see paragraph 19); or

(g) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 20).

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

5.3 The UK GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given their Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

5.4 You must discuss and identify the legal ground being relied on for each Processing activity with the DPO.

6. CONSENT

6.1 A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent. We do not generally rely on Consent as a basis for processing Personal Data therefore if you believe we require the Consent of an individual in order to process their Personal Data, please discuss this with the DPO.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

7.1 The UK GDPR requires a Controller to provide detailed, specific information to a Data Subject depending on whether the information was collected directly from the Data Subject or from elsewhere. The information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

7.2 Whenever we collect Personal Data directly from a Data Subject, including for HR or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, and how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

7.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting or receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7.4 If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice.

7.5 Any Privacy Notice must be approved by the DPO before being used.

8. PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

8.3 If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the DPO for advice on how to do this in compliance with both the law and this Data Protection Policy.

9. DATA MINIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

9.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2 You must ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after an appropriate time, unless a law requires that data to be kept for a minimum time.

11.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete that data where applicable.

11.5 You will ensure Data Subjects are provided with information about the period for which data is stored and how that period is determined in any applicable Privacy Notice.

12. SECURITY INTEGRITY AND CONFIDENTIALITY

12.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others, and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

12.3 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

12.4 You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;

(b) Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and

(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

12.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

13. REPORTING A PERSONAL DATA BREACH

13.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances, the Data Subject.

13.2 We will notify the Data Subject or any applicable regulator where we are legally required to do so following a suspected Personal Data Breach.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself and immediately contact the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

14. TRANSFER LIMITATION

14.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country. If you propose to transfer Personal Data outside the UK, please contact the DPO and follow their instructions.

15. DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 A Data Subject has rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Controller's Processing activities;

(c) request access to their Personal Data that we hold (including receiving a copy of their Personal Data);

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) object to Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

(i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(k) make a complaint to the supervisory authority;

(l) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must immediately forward any Data Subject request you receive to the DPO.

16. ACCOUNTABILITY

16.1 The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The Company must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a DPO (where necessary) or an individual accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Data Protection Policy or Privacy Notices;

(d) periodically consider the need for, and delivering if required, training Company Personnel on the UK GDPR, this Data Protection Policy, and data protection matters including, for example, a Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) periodically consider the need for, and delivering if required, regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. RECORD KEEPING

17.1 The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

18. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

18.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

18.2 You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

(a) The state of the art.

(b) The cost of implementation.

(c) The nature, scope, context and purposes of Processing.

(d) The risks of varying likelihood and severity for rights and freedoms of the Data Subject posed by the Processing.

18.3 You must involve the DPO (who will conduct a DPIA) when carrying out high-risk Processing or implementing major system or business change programs involving the Processing of Personal Data including:

(a) Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

(b) Automated Processing.

(c) Large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data.

(d) Large-scale, systematic monitoring of a publicly accessible area.

18.4 A DPIA will include:

(a) A description of the Processing, its purposes and the Controller's legitimate interests if appropriate.

(b) An assessment of the necessity and proportionality of the Processing in relation to its purpose.

(c) An assessment of the risk to individuals.

(d) The risk mitigation measures in place and demonstration of compliance.

19. DIRECT MARKETING

19.1 We are subject to certain rules and privacy laws when engaging in direct marketing to our customers and prospective customers (for example when sending marketing emails or making telephone sales calls). When carrying out direct marketing, the DPO's advice should be sought.

19.2 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

19.3 A Data Subject's objection to direct marketing must always be promptly honoured. If a customer opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

19.4 You must comply with the Company's guidelines on direct marketing to customers and you should consult the DPO if you are unsure regarding how to comply with either the Company's guidelines or the law.

20. SHARING PERSONAL DATA

20.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

20.2 You may only share the Personal Data we hold with another employee, agent or representative of our Company if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

20.3 You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains UK GDPR-approved third party clauses has been obtained.

21. CHANGES TO THIS DATA PROTECTION POLICY

21.1 We keep this Data Protection Policy under regular review. This draft was published on 01/01/2024.

22. GLOSSARY

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Company name: Agricultural & Estate Services Limited

Company Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person with responsibility for data protection compliance which at the time of publishing this policy is Mike Skinner.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: notices (either set out in this Policy as they relate to employees and contractors) or separate from this policy setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of:

(a) general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy); or

(b) stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

Data Privacy Notice for Employees, Workers and Contractors

What is the purpose of this document?

Agricultural & Estate Services Ltd (**AES, we, us, our**) is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

It applies to all employees, workers and contractors.

AES is a "controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using that information and what your rights are under the data protection legislation.

Data protection principles

We will comply with data protection law, which says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the person's identity has been removed (anonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health, sexual orientation or criminal convictions.

We will collect, store and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.

- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means.
- Information about your use of our information and communications systems.
- Photographs.
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Trade union membership.
- Information about your health, including any medical condition and sickness records, including:
    - where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill health, injury or disability, the records relating to that decision;
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
    - any health information in relation to a claim made under the permanent health insurance scheme; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. Some of the grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

- making a decision about your recruitment or appointment
- Determining the terms on which you work for us.
- Determining whether your engagement is deemed employment for the purposes of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 (ITEPA 2003) and providing you with a status determination statement in accordance with the applicable provisions of ITEPA 2003.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Providing benefits to you.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties if applicable.
- Liaising with the trustees or managers of a pension arrangement operated by us, your pension provider and any other provider of employee benefits if applicable.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.

- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations or exercise rights in connection with employment.

3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to a pension scheme.

4. Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below. We have indicated the purpose or purposes for which we are processing or will process your more sensitive personal information.

- We will use information about your physical or mental health, or disability status, to:
    - ensure your health and safety in the workplace;
    - assess your fitness to work;
    - provide appropriate workplace adjustments;
    - monitor and manage sickness absence; and
    - administer benefits including statutory maternity pay, statutory sick pay and pensions and permanent health insurance (to the extent applicable).

    We need to process this information to exercise rights and perform obligations in connection with your employment.
- If you apply for an ill-health pension under a pension arrangement operated by us we will use information about your physical or mental health in reaching a decision about your entitlement.
- If we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider

whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This is usually where that processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.

We will carry out DVLA checks and DBS checks on you from time to time as required. The reports shall be retained by us which may hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- To consider your suitability for the role
- To consider your suitability for driving vehicles in the performance of your role.

We are allowed to use your personal information in this way to carry out our obligations to customers. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Data sharing

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

Third parties includes third-party service providers (including contractors and designated agents). The following activities may be carried out by third-party service providers: payroll, pension administration, benefits provision and administration, and IT services.

We will share personal data regarding your participation in any pension arrangement operated by us with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC and disclosures to shareholders such as directors' remuneration reporting requirements.

Transferring information outside the UK

We use cloud storage which means that some of the personal information we collect about you could be transferred to countries outside the UK. We will ensure that your personal information receives and adequate level of protection and will put measure in place to ensure that the third party cloud service provider respects UK law on data protection.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available from the DPO. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Additionally, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements. Details of retention periods for different aspects of your personal information are available from the DPO.

To determine the appropriate retention period for personal data, we consider:

- The amount, nature and sensitivity of the personal data.
- The potential risk of harm from unauthorised use or disclosure of your personal data.
- The purposes for which we process your personal data and whether we can achieve those purposes through other means.

- The applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use that information without further notice to you. Once you are no longer an employee, worker or contractor of the company, we will retain and securely destroy your personal information in accordance with [our Data Retention Policy **OR** applicable laws and regulations].

Rights of access, correction, erasure and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a data subject access request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another

appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data protection officer (DPO)

We have appointed a Mike Skinner as the DPO to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO) with respect to data protection issues.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the DPO.