DATA PROTECTION POLICY & PROCEDURE

1.0 INTRODUCTION

1.1 This policy sets out the obligations of Green Element Limited and Compare Your Footprint Limited (herein collectively referred to as "the Company," "We" or "Us") regarding data protection and the rights of its employees and contractors (in this context, "Data Subjects" or "You") in respect of their Personal Data under Data Protection Law.

1.2 "Data Protection Law" means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

1.3 This policy sets out the Company's obligations regarding the collection, Processing, transfer, storage, and disposal of Personal Data relating to Data Subjects. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, and third parties working on behalf of the Company.

1.4 For ease of use, the policy is divided into a number of sections as follows:

2.0 DEFINITIONS AND INTERPRETATIONS

In this policy the following terms shall have the following meanings:

"Consent"	means the Consent of the Data Subject which must be a freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the Processing of Personal Data relating to them;
"Data Controller"	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For the purposes of this policy, the Company is the Data Controller of all Personal Data relating to employee Data Subjects;
"Data Subject"	means a living, identified, or identifiable natural person about whom the Company holds Personal Data (in this context, employee or contractor Data Subjects);
"EEA"	means the European Economic Area consisting of all EU Member States, Iceland, Liechtenstein and Norway;

"Personal Data"	means any information relating to a Data Subject who can be identified, directly, or indirectly, in particular by reference to an identifier such as a name, 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 the Data Subject;
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed;
"Processing", "Processed or "Process"	means any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and
"Special Category Personal Data"	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric or genetic data.

3.0 SCOPE

3.1 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all Data Subjects with whom it works.

3.2 The Company's Data Protection Officer is William Richardson, CEO. The Data Protection Officer is responsible for administering this policy.

3.3 All Directors and Line Managers are responsible for ensuring that all employees, agents, contractors, or third parties working on behalf of the Company comply with this policy and, where applicable, must implement such practices, Processes, controls, and training as are reasonably necessary to ensure such compliance.

3.4 Any questions relating to this policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

3.4.1 if there is any uncertainty relating to the lawful basis on which the Data Subject's Personal Data is to be collected, held, and/or Processed;

3.4.2 if Consent is being relied upon in order to collect, hold, and Process the Data Subject's Personal Data;

3.4.3 if there is any uncertainty relating to the retention period for any particular type(s) of Data Subject's Personal Data;

3.4.4 if any new or amended privacy notices or similar privacy-related documentation are required;

3.4.5 if any assistance is required in dealing with the exercise of the Data Subject's rights (including, but not limited to, the handling of a subject access request);

3.4.6 if a Personal Data Breach (suspected or actual) has occurred;

3.4.7 if there is any uncertainty relating to security measures (whether technical or organisational) required to protect the Data Subject's Personal Data;

3.4.8 if the Data Subject's Personal Data is to be shared with third parties (whether such third parties are acting as Data Controllers or data Processors);

3.4.9 if the Data Subject's Personal Data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so;

3.4.10 when any significant new Processing activity is to be carried out, or significant changes are to be made to existing Processing activities, which will require a data protection impact assessment to be carried out prior to doing so;

3.4.11 when the Data Subject's Personal Data is to be used for purposes different to those for which it was originally collected;

3.4.12 if any automated Processing, including profiling or automated decision-making, is to be carried out; or

3.4.13 if any assistance is required in complying with the law applicable to direct marketing.

4.0 THE DATA PROTECTION PRINCIPLES

4.1 This policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which anyone handling Personal Data must comply.

4.2 Data Controllers are responsible for, and must be able to demonstrate, such compliance.

4.3 All Personal Data must be:

4.3.1 Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;

4.3.2 collected for specified, explicit, and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. Further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is Processed;

4.3.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that Personal Data is inaccurate, having regard to the purposes for which it is Processed, is erased, or rectified without delay;

4.3.5 not be kept for longer than is necessary for the purposes for which it is Processed; and

4.3.6 Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

5.0 HOW WE DEFINE PERSONAL DATA

5.1 '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 expressions of opinion about the person and an indication of the intentions of Us or others, in respect of that person. It does not include anonymized data.

5.2 This policy applies to all Personal Data whether it is stored electronically, on paper, or in/on other materials. This Personal Data might be provided to the Company by You, or by someone else (such as a former employer, a former client, your doctor, or a credit reference agency for example), or it could be created by Us. It could be provided or created during the

recruitment/engagement Process or during the course of the employment contract (or contract for services) or after it has ended. It could be created by your Line Manager/client contact or other colleagues.

5.3 The Company will collect and use the following types of Personal Data about its employees:

5.3.1 Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments and documents.
5.3.2 Your contact details and date of birth.
5.3.3 Your address.
5.3.4 The contact details of your emergency contact/next of kin.
5.3.5 The contact details of your references and witness to your signature on your employment contract.
5.3.6 Your gender.
5.3.7 Your marital status and family details.
5.3.8 Information about your employment contract including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), other paid leave,
profit share bonus, staff equity, pension, benefits, deductions and leave entitlements.
5.3.9 Your time and attendance record.
5.3.10 Your expense claim record.
5.3.11 Your notice period and probation review.
5.3.12 Your exit interview record.
5.3.13 Your bank details and information in relation to your tax status including your National Insurance number.
5.3.14 Details of any student loans, CCJ's or CSA payments.
5.3.15 Details of any intellectual property made wholly or partially by you.
5.3.16 Details of any Company property provided to or owned by you.
5.3.17 Your opt-out of the Working Time Regulations and details of any secondary employment approved or refused by the Company.
5.3.18 Your identification documents such as Your passport, birth certificate and information in relation to your immigration status and right to work for the Company.
5.3.19 Information relating to disciplinary, grievance, bribery and corruption, public interest disclosure investigations and proceedings involving You (whether or not You were the main subject of those proceedings).
5.3.20 Information relating to your performance and behaviour at work.
5.3.21 Details of any incidents impacting Health & Safety.
5.3.22 Training and induction records.
5.3.23 Electronic information in relation to your use of IT systems/software/swipe cards/telephone systems.
5.3.24 Your images (whether captured by CCTV, by photograph or video)
5.3.25 Any other category of Personal Data which We may notify You of from time to time.

5.4 The Company will collect and use the following types of Personal Data about its contractors/agents:

5.4.1 Your contact details.
5.4.2 Engagement information such as your registered office/address and VAT registration number.
5.4.3 Information about your contract for services including start and end dates, services provided, term of agreement, payment terms and indemnification.
5.4.4 Your expense claim record.
5.4.5 Your acknowledgement of Company policies that apply to contractors/agents.

5.4.6 Details of any intellectual property made wholly or partially by you.
5.4.7 Details of any Company property provided to or owned by you.
5.4.8 Information relating to your performance and behaviour at work.
5.4.9 Electronic information in relation to your use of IT systems/software/swipe cards/telephone systems.
5.4.10 Your images (whether captured by CCTV, by photograph or video)
5.4.11 Any other category of Personal Data which We may notify You of from time to time.

6.0 HOW WE DEFINE SPECIAL CATEGORIES OF PERSONAL DATA

6.1 'Special Categories of Personal Data' are types of Personal Data consisting of information about:

6.1.1 Your racial or ethnic origin;
6.1.2 Your political opinions;
6.1.3 Your religious or philosophical beliefs;
6.1.4 Your trade union membership;
6.1.5 Your genetic or biometric data;
6.1.6 Your health; and
6.1.7 Your sexual orientation.

6.2 We may hold and use any of these special categories of your Personal Data in accordance with the law.

7.0 HOW WE DEFINE PROCESSING

7.1 'Processing' means any operation which is performed on Personal Data such as:

7.1.1 collection, recording, organisation, structuring or storing;
7.1.2 adaption or alteration;
7.1.3 retrieval, consultation, or use;
7.1.4 disclosure by transmission, dissemination or otherwise making available;
7.1.5 alignment or combination; and
7.1.6 restriction, destruction, or erasure.

7.2 This includes Processing Personal Data which forms part of a filing system and any automated Processing.

8.0 HOW WILL WE PROCESS YOUR PERSONAL DATA?

8.1 We will Process Your Personal Data (including Special Categories of Personal Data) in line with our obligations under the 2018 Act.

8.2 We will use your Personal Data:

8.2.1 for performing the employment contract (or contract for services) between Us;
8.2.2 for complying with any legal obligation; or
8.2.3 if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, We can only do this if your interests and rights do not

override ours (or theirs). You have the right to challenge our legitimate interests and request that We stop this Processing.

8.3 We can Process your Personal Data for these purposes without your knowledge or Consent. We will not use your Personal Data for an unrelated purpose without telling You about it and the legal basis that We intend to rely on for Processing it.

8.4 If You choose not to give Us certain Personal Data, We may not be able to carry out some parts of the contract between Us. For example, if We do not have your bank account details, We may not be able to pay You. It might also prevent Us from complying with certain legal obligations and duties, such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability You may have/develop.

9.0 EXAMPLES OF WHEN WE MIGHT PROCESS YOUR PERSONAL DATA

9.1 We have to Process Your Personal Data in various situations during your recruitment, employment (or engagement) and even following termination of your employment.

9.2 For example:

9.2.1 to decide whether to employ (or engage) You;
9.2.2 to decide how much to pay You, and the other terms of your contract or contract for services with Us;
9.2.3 to check You have the legal right to work for Us;
9.2.4 to carry out the contract between Us including; where relevant, its termination;
9.2.5 to train You and review your performance*;
9.2.6 to decide whether to promote You;
9.2.7 to decide whether and how to manage your performance, absence or conduct*;
9.2.8 to carry out a disciplinary or grievance investigation or procedure in relation to You or someone else;
9.2.9 to determine whether We need to make reasonable adjustments to your workplace or role because of your disability*;
9.2.10 to monitor diversity and equal opportunities*;
9.2.11 to monitor and protect the security (including network security) of the Company, You, other Staff, clients and third parties;
9.2.12 to monitor and protect the health and safety of You, other staff, clients and third parties*;
9.2.13 to pay You and provide pension and other benefits in accordance with the contract between Us*;
9.2.14 to pay tax and National Insurance;
9.2.15 to provide a reference upon request from another employer;
9.2.16 to pay trade union subscriptions, Student Loans, CCJ's, CSA payments on your behalf*;
9.2.17 to monitor compliance by You, Us and others with our policies and our contractual obligations*;
9.2.18 to comply with employment law, immigration law, health and safety law, tax law and other laws which affect Us*;
9.2.19 to answer questions from insurers or benefit providers in respect of any insurance or benefit policies which relate to You*;
9.2.20 to run our business and plan for the future;
9.2.21 for the prevention and detection of fraud or other criminal offences;
9.2.22 to defend the Company in respect of any investigation or litigation and to comply with any court of tribunal orders for disclosure*; and
9.2.23 for any other reason which We may notify You of from time to time.

9.3 We will only Process Special Categories of your Personal Data in certain situations in accordance with the law. For example, We can do so if We have your explicit Consent. If We ask for your Consent to Process a special category of Personal Data then We will explain the

reasons for our request. You do not need to Consent and can withdraw Consent at a later stage by contacting the Data Protection Officer.

9.4 We do not need your content to Process Special Categories of your Personal Data when We are Processing it for the following purposes:

9.4.1 Where it is necessary for carrying out rights and obligations under employment law.
9.4.2 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.
9.4.3 Where You have made the data public.
9.4.4 Where Processing is necessary for the establishment, exercise, or defence of legal claims.
9.4.5 Where Processing is necessary for the purposes of occupational health or for the assessment of your working capacity.

9.5 We might Process Special Categories of your Personal Data for the purposes in clause 9.2 which have an * beside them. In particular, We will use information in relation to:

9.5.1 Your race, ethnic origin, religion, sexual orientation, or gender to monitor equal opportunities;

9.5.2 Your sickness absence, health, and medical conditions to monitor your absence, assess your fitness for work, to pay You benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and

9.5.3 Your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

9.6 We do not take automated decisions about You using your Personal Data or use profiling in relation to You.

10.0 SHARING YOUR PERSONAL DATA

10.1 Sometimes We might share your Personal Data with our contractors and agents to carry out our obligations under our contract with You or for our legitimate interests.

10.2 We require those people and companies to keep your Personal Data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to Process your Personal Data for the lawful purpose for which it has been shared and in accordance with our instructions.

10.3 The legitimate interests that our third parties undertake on our behalf are:

10.3.1 Accountancy and payroll services provided by our external providers in order to pay You; deduct income tax; make National Insurance contributions; deduct student loans/CCJ's/CSA payments; make payments to your Company pension; reimburse you for Company expenses; and allocate/record your working time.

10.3.2 People Operations services provided by our external HR Consultant in order to provide support to employees and management in all aspects of the contractual and legal relationship between Us and You during the employee lifecycle.

10.3.3 IT services provided by our external IT and software consultants in order to provide IT equipment and software support to the Company that you have access to and use to perform your responsibilities.

10.4 We do not send your Personal Data outside of the EEA. If this changes, We will tell You. We will also explain the protections that are in place to protect the security of your data.

10.5 In the event that a third-party advises us that they have commenced sending your Personal Data outside of the EEA as part of the service that they provide to Us then We will advise You of this and follow the necessary processes/get relevant assurances that such data is being stored and processed as per the appropriate legal requirements.

11.0 HOW SHOULD YOU PROCESS PERSONAL DATA FOR THE COMPANY?

11.1 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 and other relevant policies in place from time to time.

11.2 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 Personal Data for the specified lawful purpose for which it was obtained.

11.3 You should not share Personal Data informally. You should keep Personal Data secure and not share it with unauthorised people. You should regularly review and update Personal Data which You have to deal with for work. This includes telling Us if your own contact details change.

11.4 You should not make unnecessary copies of Personal Data and should keep and dispose of any copies securely.

11.5 You should use strong passwords.

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

11.7 Consider anonymising data or using separate keys/codes so that the Data Subject cannot be identified.

11.8 Do not save Personal Data to your own personal computers or other devices.

11.9 Personal Data should never be transferred outside the EEA except in compliance with the law and without prior authorisation of the Data Protection Officer.

11.10 You should lock drawers and filing cabinets to ensure that Personal Data is always kept secure.

11.11 You should not take Personal Data away from Company premises without authorisation from your Line Manager or the Data Protection Officer.

11.12 Personal Data should be shredded and disposed of securely when you have finished with it.

11.13 You should ask for help from the Company's Data Protection Officer if You are unsure about data protection or if You notice any areas of data protection or security We can improve upon.

11.14 Any deliberate or negligent breach of this policy by You may result in disciplinary action being taken against You under the Company's Disciplinary Policy.

11.15 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 Policy.

12.0 DATA PROTECTION IMPACT ASSESSMENT

12.1 The Company will carry out a Data Protection Impact Assessment before it Processes new Personal Data when the Processing is likely to result in a high risk to the rights and freedoms of Data Subjects.

12.2 Processing that is likely to result in a high risk includes (but is not limited to):

12.2.1 systematic and extensive Processing activities, including profiling and where decisions that have legal effects, or similarly significant effects, on individuals;

12.2.2 large scale Processing of special categories of data or Personal Data relating to criminal convictions or offences;

12.2.3 using new technologies (for example introducing surveillance systems).

12.3 The Company will take into account the nature, scope, context, and purposes of the Processing when deciding whether or not it is likely to result in a high risk to Data Subject's rights and freedoms.

12.4 In the event that the Company carries out a Data Protection Impact Assessment that identifies a high risk that cannot be reduced in any way, then the Company will consult with the Information Commissioner's Office (www.ico.org.uk) prior to Processing that Personal Data.

12.5 Data Protection Impact Assessments will be conducted in accordance with the 'Data Impact Assessment Form Template' as referenced in Appendix 2 of this policy or an appropriate template provided by the Information Commissioner's Office ('ICO').

13.0 PERSONAL DATA BREACHES

13.1 If this policy is followed, the Company should not have any Personal Data Breaches. If a breach of Personal Data occurs (whether in respect of You or someone else) then the Company must take notes and keep evidence of that Personal Data Breach.

13.2 If the Personal Data Breach is likely to result in a risk to the rights and freedoms of individuals then the Data Protection Officer must also notify the ICO within 72 hours, where feasible.

13.3 If You are aware of a Personal Data Breach You must contact the Data Protection Officer immediately and keep any evidence You have in relation to the breach.

13.4 Data breaches will be managed via the advice provided in Appendix 2 of this policy ('Taking action in the case of a Personal Data Breach').

14.0 SUBJECT ACCESS REQUESTS

14.1 Data Subjects can make a 'subject access request' ('SAR') to find out what information the Company holds about them.

14.2 This request must be made in writing to the Data Protection Officer who will coordinate the response.

14.3 To make a SAR in relation to your own Personal Data, You should write to the Data Protection Officer. The Company will respond within one month unless the request is complex in which case this timeframe may be extended by up to two months.

14.4 There is no fee for making a SAR. However, if Your request is manifestly unfounded or excessive the Company may charge a reasonable administrative fee or refuse to respond to Your request.

14.5 The Company normally works on the basis that any request which will take more than one day to deal with is likely to be manifestly excessive, and in those circumstances the Company has the right to impost a reasonable charge of one working day's salary for You.

15.0 YOUR DATA SUBJECT RIGHTS

15.1 You have the right to information about what Personal Data We Process, how and on what basis as set out in this policy.

15.2 You have the right to access your own Personal Data by way of a SAR.

15.3 You can correct any inaccuracies in your Personal Data by contacting the Data Protection Officer.

15.4 You have the right to request that We erase your Personal Data where We were not entitled under law to Process it, or where it is no longer necessary to Process the Personal Data for the purpose for which it was collected. You can request erasure by contacting the Data Protection Officer.

15.5 During the Process of requesting that your Personal Data is corrected or erased, or while You are contesting the lawfulness of our Processing, You can ask for the data to be used in a restricted way only. To do this, contact the Data Protection Officer.

15.6 You have the right to object to data Processing where We are relying on a legitimate interest to do so and You think that your rights and interests outweigh our own and You wish Us to stop.

15.7 You have the right to object if We Process your Personal Data for the purposes of direct marketing.

15.8 You have the right to receive a copy of your Personal Data and, with some exceptions, to transfer your Personal Data to another Data Controller. We will not charge for this and will in most cases aim to do this within one month.

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

15.10 You have the right to be notified of a data security breach concerning your Personal Data where that breach is likely to result in a high risk of adversely affecting your rights and freedoms.

15.11 In most situations We will not rely on your Consent as a lawful ground to Process your data. If We do 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 the Data Protection Officer.

15.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly (www.ico.org.uk). This website also has more information on your rights and our obligations in respect of your Personal Data.

16.0 DATA RETENTION

16.1 There are two types of retention period's applicable to Personal Data:

a) Records where there are UK statutory retention periods.
b) Recommended retention periods where there are no UK statutory periods.

16.2 Examples of statutory retention periods are summarised below. If in doubt, keeping records for at least 6 years (5 in Scotland), covers the standard time limit for any civil legal action.

16.2.1 Accident books, accident records/reports- 3 years from the last entry (or until any younger person involved in the accident reaches 21).
16.2.2 Accounting records- 3 years for private companies.
16.2.3 First aid training- 6 years after employment.
16.2.4 Fire Warden training- 6 years after employment.
16.2.5 Health and Safety representatives and employees' training- 5 years after employment.
16.2.6 Income tax and NI returns, income tax records and correspondence with HMRC- Not less than 3 years after the end of the relevant financial year.
16.2.7 Medical records, tests and examinations of control systems such as those specified by COSHH, Control of Asbestos Regulations etc- 40 years from the date of the last entry.
16.2.8 National minimum wage records- 3 years after the end of the pay reference period following the one that the records cover.
16.2.9 Payroll wage/salary records (also overtime, bonuses, expenses)- 6 years from the end of the tax year to which they relate.
16.2.10 Records relating to children and young adults- until the child/young adult reaches the age of 21.
16.2.11 Retirement Benefits Schemes- 6 years from the end of the scheme year in which the event took place.
16.2.12 Statutory Maternity Pay records including Mat B1s (also shared parental, paternity and adoption pay records)- 3 years after the end of the tax year in which the maternity period ends.
16.2.13 Subject access request- 1 year following completion of the request.
16.2.14 Whistleblowing documents- 6 months following the outcome (if a substantiated investigation). If unsubstantiated, Personal Data should be removed immediately.
16.2.15 Working time records including overtime, annual holiday, time off for dependents, etc- 2 years from date on which they were made.

16.3 For many types of employment records, there is no definitive retention period therefore the following are recommending:

16.3.1 Pension actuarial valuation reports- Permanently.
16.3.2 Assessments under health and safety regulations and safety representatives and committee records (including previous COVID-19 risk assessments)- Permanently.
16.3.3 Collective agreements- 6 years after the agreement ends.
16.3.4 COVID-19 vaccination records – this is 'special category' data requiring extra protection. Employers can only keep this data for a good reason and if there is a lawful basis for Processing it such as employee or public health.
16.3.5 CCTV footage- 6 months following the outcome of any formal decision or appeal. CCTV footage may be relevant to a disciplinary matter or unfair dismissal claim.

16.3.6 Driving offences- Must be removed once the conviction is spent under the Rehabilitation of Offenders Act 1974.
16.3.7 Flexible working requests- 18 months following any appeal. This is because a further request cannot be made for 12 months following a request plus allowing for a 6 month tribunal limitation period on top.
16.3.8 Inland Revenue/HMRC approvals- Permanently.
16.3.9 Parental leave- 18 years from the birth of the child.
16.3.10 Pension records- 12 years after the benefit ceases.
16.3.11 Pension scheme investment policies- 12 years from the ending of any benefit payable under the policy.
16.3.12 HR files and training records (including disciplinary and working time records)- 6 years after employment ceases but may be unreasonable to refer to expired warnings after two years have elapsed.
16.3.13 Recruitment application forms and interview notes (for unsuccessful candidates)- 6 months to a year. Because of the time limits in the Equality Act, relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants' documents will transfer to the personnel file.
16.3.14 Redundancy details, calculations of payments, refunds, notification to the Secretary of State- 6 years from the date of redundancy.
16.3.15 References- At least one year after the reference is given to meet the limitation period for defamation claims.
16.3.16 Right to work in the UK checks- Home Office recommended practice is 2 years after employment ends.
16.3.17 Senior executives' records (senior management team or equivalents- Some records may need permanent retention such as documents from the company's incorporation, shareholdings, resolutions, memorandum and articles, annual returns, register of directors interests, share documents, accounts, liability policies, pension scheme documents etc most of which should be retained permanently. Retain personal records, performance appraisals, employment contracts etc for 6 years after the employee has left to reflect the main limitation period.
16.3.18 Statutory Sick Pay (SSP) records, calculations, certificates, self-certificates, occupational health reports. Also COVID-19-related SSP records such as the dates off sick- Six months after the end of the period of sick leave is sensible in case of a disability discrimination claim. For personal injury claims, the limitation is 3 years. If there's a contractual claim for breach of an employment contract then keep records for 6 years after the employment ceases. Employers should keep a record of SSP paid due to COVID-19 as HMRC may request records.
16.3.19 Termination of employment, for example early retirement, severance or death in service- at least 6 years.
16.3.20 Terms and conditions including offers, written particulars, and variations- 6 years after employment ceases or the terms are superseded.
16.3.21 Trade union agreements- 10 years after ceasing to be effective.
16.3.22 Trust deeds and rules- permanently.
16.3.23 Trustees' minute books- permanently.
16.3.24 Works council minutes- permanently.

17.0 ACCOUNTABILITIES

17.1 The CEO has the overall responsibility of ensuring the Company and its representatives adhere to this policy.

17.2 People Operations has the responsibility of ensuring this policy is reviewed and updated as and when relevant legal updates occur.

17.3 Employees and contractors have the responsibility of ensuring that Personal Data kept or seen during the course of conducting their duties is done so in line with the requirements stipulated within this policy in addition to reporting to the Data Protection Officer any breach, whether suspected or otherwise, of Personal Data.

APPENDIX 1- Data Protection Impact Assessment Template

This template is an example of how to record a Data Protection Impact Assessment (DPIA) process and outcome. It follows the process set out in the DPIA guidance created by the Information Commissioner's Office (www.ico.org.uk).

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA
Explain broadly what the project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA.
Step 2: Describe the processing
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it is not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Describe the processing			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm.** Remote, possible, or probable	**Severity of harm.** Minimal, significant, or severe	**Overall risk.** Low, medium, or high

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk.** Eliminated, reduced or accepted.	**Residual risk.** Low, medium or high.	**Measure approved.** Yes/No

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
Data Protection Officer (DPO) advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX 2- Taking action in the case of a Personal Data Breach

The following guidance should be referred to in the case of a Personal Data Breach, whether suspected or known. Personal Data Breaches can be as simple as someone sending an email to the wrong person or more complex such as a Company laptop being stolen from a car or a cyberattack on Company systems.

Further details on managing a Personal Data Breach is available from the specific sections relating to, and the reporting of, a Personal Data Breach on the Information Commissioner's Officer website (www.ico.org.uk) which the below advice is taken from.

Step one: Don't panic
It is understandable if you are concerned about what happens next however, it is important to quickly understand what has happened and to prevent it from happening again.

Step two: Start the timer
By law, the DPO has to report a personal data breach to the ICO (www.ico.org.uk) without undue delay (if it meets the threshold for reporting) and within 72 hours.

The Company might end up not needing to report it, but start a log anyway, to record what happened, who is involved and what you are doing about it. The clock starts from when you discovered the breach, not when it actually happened.

Step three: Find out what has happened
Pull the facts together as quickly as possible. Write down facts about the incident as you uncover them. This could be things like what happened and why, how many people were involved, a timeline of when it all happened, and what actions you have taken so far.

Step four: Try to contain the breach
Your priority is to establish what has happened to the Personal Data affected. If you can recover the Personal Data, do so immediately. Also you should do whatever you can to protect those who will be most impacted.

For example, if the Personal Data has been sent to someone by mistake, you could ask them to delete it, send it back securely, or have it ready for you to collect.

If you are dealing with a stolen laptop and the Company has the appropriate systems installed, wipe it remotely. This will help to minimise the risk of personal data falling into the wrong hands.

You could contain a cyber incident by changing all passwords and making sure your staff do the same.

If you need help thinking of other ways to contain the breach, contact the ICO for further advice.

Step five: Assess the risk
Assess what you feel the risk of harm is to those affected, whether that's your employees, contractors, clients, members or service users.

By risk of harm, we mean any potential harm or detriment it may cause to people, eg safeguarding issues, identity theft or significant distress. You might be dealing with a simple mix-up where there is little or no risk involved, or a serious breach that will have a lasting effect on people's lives.

When assessing risk, it can help to put yourself into the shoes of those who have been impacted.

For example, supposing you email an appointment reminder to the wrong client and they have deleted the email. If you were the client you meant to remind, would you be worried? Unless there is more to this than meets the eye, it is unlikely you would need to tell the customer or the ICO.

Step six: If necessary, act to protect those affected
If possible, you should give specific and clear advice to people on the steps they can take to protect themselves, and what you are willing to do to help them. If you do not think there's a high risk to the people involved, you don't have to let them know about the incident.

Now that you have established what happened, tried to contain the breach and assessed the risk of harm to those who have been affected, your next step is to do what you can to protect them further.

Depending on the circumstances, this may include advising people to use strong, unique passwords, telling them to look out for phishing emails or fraudulent activity on their accounts and providing guidance on protecting themselves from identity theft.

There is nothing stopping you telling people about the incident, even if you do not think there's a high risk to them, but you'll want to balance any risk to them against the potential of causing unnecessary worry.

If you think there is a high risk, then by law you have to tell them without undue delay. For example, if you feel there is a high risk of them having their identity stolen, then you have to let them know so they can be extra vigilant and take steps to protect themselves.

Step seven: Submit your report (if needed)
If the breach is reportable, call the ICO reporting helpline, on 0303 123 1113 available Monday to Friday, 9am to 5pm.

If you're unsure if your breach is reportable you can also use the ICO's self-assessment tool to help you decide or you can call our personal data breach advice line.

When you report a breach, you'll need to provide details such as what happened and when, your risk assessment, and what you've done to contain the breach. Please be ready to provide as much information as you can. This will help us give you the most relevant advice for the next steps you should take.

Don't worry if you haven't got all the information to hand straight away – the important part is letting us know that it's happened before 72 hours have passed. You can always provide more later as part of a follow-up report if necessary. This should be completed without undue delay and should be an urgent priority for you.