Data Protection and Data Security Policy

1 STATEMENT AND PURPOSE OF POLICY

Luce Bay Group are committed to ensuring that all personal information handled by us will be processed accordingly to legally compliant standards of data protection and data security in accordance with the Data Protection Act 2018.

The purpose is of this policy is to help us achieve our data protection and data security aims by:

- Notifying individuals of the types of personal information that we may hold about them and what we do with that information;
- Ensuring staff understand our rules and legal standards for handling personal information relating to others: and
- Clarifying the responsibilities and duties of staff in respect of data protection and data security.

This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

2 WHO IS RESPONSIBLE FOR DATA PROTECTION AND DATA SECURITY?

Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed term staff and any volunteers (staff).

The Directors have overall responsibility for ensuring that all personal information is handled in compliance with the law.

All staff have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out here and to ensure that measures are taken to protect data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance.

Any breach of this policy will be taken seriously and may result in disciplinary action.

3 WHAT PERSONAL INFORMATION AND ACTIVITIES ARE COVERED BY THIS POLICY?

This policy covers personal information:

- which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess
- which relates to staff (present, past or future) or to any other individual whose personal information we handle or control
- which we obtain, hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

4 WHAT PERSONAL INFORMATION DO WE PROCESS AND WHAT DO WE DO WITH IT?

We collect personal information about you which:

- You provide or we gather before or during your employment or engagement with us
- Is provided by third parties, such as references or information from suppliers or another party we do business with
- Is in the public domain

The types of personal information that we may collect, store and use about you include records relating to your:

- Home address and contact details as well as contact details for your next of kin;
- Recruitment (including your application form or cv, any references and received and details of your qualifications);
- Pay records, national insurance number and details of your taxes and any employment benefits such as pension, health insurance (including details of any claims made);
- Any sickness absence or medical information provided;
- Religious or philosophical beliefs (eg specific dietary or holiday requirements);
- Sexual orientation, where this is disclosed to us (eg through providing details of your spouse or partner for the administration of benefits);
- A telephone, email, internet, fax or instant messenger use;
- Performance and any disciplinary matters, grievances, complaints or concerns in which you are involved in.

We will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have including:

- **Staff Address Lists:** to compile and circulate lists of home addresses and contact details, to contact you outside working hours.
- **Sickness Records**: to maintain a record of your sickness absence and copies of any doctors notes or other documents supplied to us in connection with your health, to inform your colleagues and others of that you are absent through your sickness, as

reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.

- **Disciplinary, grievance or legal matters**: in connection with any disciplinary, grievance, legal, regulatory or compliance maters or proceedings that may involve you.
- **Performance Reviews**; to carry out performance reviews.

5 We confirm that for the purpose of the Data Protection Act 2018, the employer is a data controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal information is processed.

6 If you consider that any information held about you is inaccurate then you should tell your line manager, if we agree that the information is inaccurate then we will correct it. If we do not agree with the correction then we will note your comments.

7 We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside the employer. However, we may need to disclose personal information about Staff:

- For the administration of your employment and associated benefits e.g. to the providers of our pension or insurance schemes;

  Or
- To comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to employment issues, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities, such has HM Revenue and Customs;
- To other parties which provide products or services to us.

8 By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

9 DATA PROTECTION PRINCIPLES

Staff whose work involves using personal data relating to others must comply with this policy and with the eight legal data protection principles which require that personal information is:

- **Processed fairly and lawfully**. We must always have a lawful basis to process personal information. In most (but not all) cases, the person to whom the information relates (the subject) must have given consent. The subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.

- **Processed for limited purposes and in an appropriate way**. Personal information must not be collected for one purpose and then used for another. If we want to change the way we use personal information we must first tell the subject.
- **Adequate, relevant and not excessive for the purpose**.
- **Accurate**. Regular checks must be made to correct or destroy inaccurate information.
- **Not kept longer than necessary for the purpose**. Information must be destroyed or deleted when we no longer need it. For guidance on how long particular information should be kept, contact the Data Protection Officer.
- **Processed in line with Subjects rights**. Subjects have a right to request access to their personal information, prevent their personal information being used for direct-marketing, and request the correction of inaccurate data to prevent their personal information being used in a way likely to cause them or another person damage or distress.
- **Secure**. See further information about data security below.
- **Not transferred to people or organisations situated in countries without adequate protection**.

10 Some personal information needs even more careful handling. This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life or about criminal offences. Strict conditions apply to processing this sensitive personal information and the subject must normally have given specific and express consent to each way in which the information is used.

11 DATA SECURITY

We must all protect personal information in our possession from being accessed, lost, deleted or damaged unlawfully or without proper authorisation through the use of data security measures.

12 Maintaining data security means making sure that:

- Only people who are authorised to use the information can access it;
- Information is accurate and suitable for the purpose for which it is processed; and
- Authorised persons can access information if they need it for authorised purposes. Personal information therefore should not be stored on individual computers but instead on our central system.

13 By law we must use procedures to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

14 Personal information must not be transferred to any person to process (eg while performing services for us on our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

15 SECURITY PROCEDURES INCLUDE:

- **Physically securing information.** Any desk or cupboard containing confidential information must be kept locked. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
- **Controlling access to premises.** Staff should report to the director if they see any persons they do not recognise trying to gain access to the property.

16 TELEPHONE PRECAUTIONS

Particular care must be taken by staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

- The identity of any telephone caller must be verified before any personal information is disclosed;
- if the callers identity cannot be verified satisfactorily then they should be asked to put their query in writing;
- Do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the company director.

17 METHODS OF DISPOSAL

Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

18 SUBJECT ACCESS REQUESTS

By law, any Subject (including Staff) may make a formal request for information that we hold about them, provided that certain conditions are met. The request must be made in writing. A fee may be payable by the data subject for provision of this information. In some circumstances it may not be possible to release the information about the subject to them e.g. if it contains personal data about another person.

Adam McIntosh
Company Director
01 December 2024

Alastair McIntosh
Company Director
01 December 2024