DATA BACKUP PROCEDURE

1. Scope

All Blakeney Leigh Limited all records whether analogue or digital, are subject to the retention requirements of this procedure.

2. Responsibilities

2.1 The following roles are responsible for retention of these records because they are the information asset owners.
2.2 Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.
2.3 The Data Protection Officer is responsible for storage of data in line with this procedure.
2.4 The Directors are responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

3. Procedure

3.1 The required retention periods, by record type, are recorded in the Retention of Records under the following categories:
- 3.1.1 Record type
- 3.1.2 Retention period
- 3.1.3 Retention period to start from (at creation, submission, payment, etc.)
- 3.1.4 Retention justification
- 3.1.5 Record medium
- 3.1.6 Disposal method

3.2 Each data asset that is stored is marked with the name of the record, the record type, the original owner of the data, the information classification, the data of storage, the required retention period, the planned date of destruction, and any special information.
3.3 For all storage media (electronic and hard copy records), The Company retains the means to access that data.
3.4 For all electronic storage media, The Company does not exceed 90% of the manufacturer's recommended storage life. This is recorded in the Log of Information Assets for Disposal. When the maximum is reached, the stored data is copied onto new storage media.
3.5 The procedure for accessing stored data is detailed in Access Control Rules and Rights for Users/User Group
3.6 The Data Protection Officer is responsible for destroying data once it has reached the end of the retention period as specified in Retention and Disposal Schedule. Destruction must be completed within 30 days of the planned retention period.
3.7 Portable/removable storage media are destroyed

Signature:  Date 30.06.25

DATA DISPOSAL PROCEDURE

1. Scope

Blakeney Leigh Limited requires that all removable storage media are clean (which means it is not possible to read or reconstitute the information that was stored on the device or document) prior to disposal.

2. Responsibilities

2.1 The Information Security Manager is responsible for managing the secure disposal of all storage media in line with this procedure when they are no longer required.

2.2 All owners of removable storage media are responsible for ensuring that these media are disposed of in line with this procedure.

3. Procedure

3.1 Hard disks must be cleared of all software and all organisational information prior to disposal or reuse, as set out in Clause 3.5 and 3.6, below.

- 3.1.1 In the event that hard disks/media contain personal data, and it cannot be removed, then:
  - 3.1.1.1 Review whether or not you really do need to keep an archive within which this personal data is stored; it may well be that there is no overriding business reason for the archive in the first place.
  - 3.1.1.2 If you currently cannot technically delete archived data that is beyond its retention date, then to the hard disk/media needs to be put securely beyond use.

3.2 The Information Security Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment is routed through their office. A log is retained showing what media were destroyed and/or disposed of, and when. The information asset inventory and/or data inventory is adjusted once the asset has been disposed of.

3.3 Hard disks are cleaned

3.4 Devices containing confidential information are destroyed prior to disposal and are never reused.

3.5 Devices containing information that are damaged are subject to a risk assessment prior to sending for repair, to establish whether they should be repaired or replaced.

3.6 Portable or removable storage media of any description are destroyed prior to disposal.

3.7 Documents containing confidential information that are to be destroyed are shredded and an approved contractor removes the waste.

Signature: 

Date 30.06.24

DATA PROTECTION POLICY STATEMENT

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 Definitions used by the Company (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.

1.3 Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on 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.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy statement

2.1 The Directors of Blakeney Leigh Limited are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information we collect and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy along with connected processes and procedures.

2.3 The GDPR and this policy apply to all personal data processing functions, including those performed on customers', clients', employees', suppliers' and partners' personal data, and any other personal data the Company processes from any source.

2.4 John Ottley is responsible for reviewing the register of processing annually in the light of any changes to our activities (as determined by changes to the data inventory register and

the management review) and to any additional requirements identified by means of data protection impact assessments.

2.5 This policy applies to all Employees. Any breach of the GDPR will be dealt with under our disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.6 Partners and any third parties working with or for the Company, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Company without having first entered into a data confidentiality agreement which imposes on the third party obligations no less onerous than those to which we are committed, and which gives the Company the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 The Company is a data processor under the GDPR.

3.2 The Directors and all those in managerial or supervisory roles throughout the Company are responsible for developing and encouraging good information handling practices; responsibilities are set out in individual job descriptions.

3.3 Data Protection Officer/GDPR Owner (Data Protection Officer (DPO) Job Description and Data Protection Job Description Responsibilities, a role specified in the GDPR, should be a member of the senior management team, is accountable to the Directors for the management of personal data and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 Development and implementation of the GDPR as required by this policy; and

3.3.2 Security and risk management in relation to compliance with the policy.

3.4 Data Protection Officer, who the Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for the Company's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the Company complies with the GDPR, as do Managers in respect of data processing that takes place within their area of responsibility.

3.5 The Data Protection Officer/GDPR Owner have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all Employees/Staff of the Company who process personal data.

3.7 The Company's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees of The Company generally.

3.8 Employees of Blakeney Leigh Limited are responsible for ensuring that any personal data about them and supplied by them to the Company is accurate and up-to-date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Our policies and procedures are designed to ensure compliance with the principles.

4.1 <u>Personal data must be processed lawfully, fairly and transparently</u>

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 The identity and the contact details of the controller and, if any, of the controller's representative;
4.1.2 The contact details of the Data Protection Officer;
4.1.3 The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.4 The period for which the personal data will be stored;
4.1.5 The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
4.1.6 The categories of personal data concerned;
4.1.7 The recipients or categories of recipients of the personal data, where applicable;
4.1.8 Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
4.1.9 Any further information necessary to guarantee fair processing.

4.2 <u>Personal data can only be collected for specific, explicit and legitimate purposes</u>
Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of the Company's GDPR register of processing.

4.3 <u>Personal data must be adequate, relevant and limited to what is necessary for processing</u>

4.3.1 The Data Protection Officer is responsible for ensuring that the Company does not collect information that is not strictly necessary for the purpose for which it is obtained.
4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be include a fair processing statement or link to privacy statement and approved by the Data Protection Officer.
4.3.3 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 <u>Personal data must be accurate and kept up to date with every effort to erase or rectify without delay</u>

4.4.1 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the data subject to ensure that data held by the Company is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4 Employees should be required to notify the Company of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained. It is the responsibility of the Company to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by the Company, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose.

4.4.7 The Data Protection Officer is responsible for responding to requests for rectification from data subjects within one month This can be extended to a further two months for complex requests. If the Company decides not to comply with the request, the Data Protection Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

4.4.8 The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5 <u>Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.</u>

4.5.1 Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach.

4.5.2 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 <u>Personal data must be processed in a manner that ensures the appropriate security</u>
The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of the Company controlling or processing operations.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the Company itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the Company's premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies;
- Identifying appropriate international security standards relevant to the Company.

When assessing appropriate organisational measures the Data Protection Officer / GDPR Owner will consider the following:

- The appropriate training levels throughout the Company;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 <u>The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)</u>

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

The Company will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
5.1.2 To prevent processing likely to cause damage or distress.
5.1.3 To prevent processing for purposes of direct marketing.
5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.
5.1.5 To not have significant decisions that will affect them taken solely by automated process.
5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.
5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.
5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
5.1.10 To object to any automated profiling that is occurring without consent.

5.2 Blakeney Leigh Limited Limited ensures that data subjects may exercise these rights:
5.2.1 Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how the Company will ensure that its response to the data access request complies with the requirements of the GDPR.
5.2.2 Data subjects have the right to complain to the Company related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure

6. Consent

6.1 The Company understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.
6.2 The Company understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation.
6.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.
6.5 In most instances, consent to process personal and sensitive data is obtained routinely by the Company using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.
6.6 Where the Company provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

7. Security of data

7.1 All Employees/Staff are responsible for ensuring that any personal data that the Company holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the Company to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, password protected in line with corporate requirements or
- Stored on (removable) computer media, which are encrypted in line with Secure Disposal of Storage Media.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees the Company. All Employees are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support.

7.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

8. Disclosure of data

8.1 The Company must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Company's business.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

9. Retention and disposal of data

9.1 The Company shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 The Company may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations the Company has to retain the data.

9.4 The Company data retention and data disposal procedures apply in all cases.

9.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

10. Data transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.

10.1.2 Privacy Shield

If the Company wishes to transfer personal data from the EU to an organisation in the United States it should check that the Company is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not.

<u>Assessment of adequacy by the data controller</u>

In making an assessment of adequacy, the UK based exporting controller should take account of the following factors:

- The nature of the information being transferred;
- The country or territory of the origin, and final destination, of the information;
- How the information will be used and for how long;
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- The security measures that are to be taken as regards the data in the overseas location.

10.1.3 Binding corporate rules

The Company may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that the Company is seeking to rely upon.

10.1.4 Model contract clauses

The Company may adopt approved model contract clauses for the transfer of data outside of the EEA.

10.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Information asset register/data inventory

11.1 The Company has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. The Company's data inventory and data flow determines:

- Business processes that use personal data;
- Source of personal data;
- Volume of data subjects;
- Description of each item of personal data;
- Processing activity;
- Maintains the inventory of data categories of personal data processed;
- Documents the purpose(s) for which each category of personal data is used;
- Recipients, and potential recipients, of the personal data;
- The role of the Company throughout the data flow;
- Key systems and repositories;
- Any data transfers; and
- All retention and disposal requirements.

11.2 Blakeney Leigh Limited Limited is aware of any risks associated with the processing of particular types of personal data.

11.2.1 The Company assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs)

are carried out in relation to the processing of personal data by the Company, and in relation to processing undertaken by other organisations on behalf of the Company.

11.2.2 The Company shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that The Company is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not The Company may proceed must be escalated for review to the Data Protection Officer.

11.2.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

11.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to The Company's documented risk acceptance criteria and the requirements of the GDPR.

Signature:  Date 30.06.24

INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

1. Scope

All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and owners of Blakeney Leigh Limited information and personal data assets or systems are required to be aware of and to follow this procedure.

2. Responsibilities

2.1 Users and owners of company information and personal data assets are required to follow this procedure for reporting information security events, weaknesses and personal data breaches, and this is documented in User Agreements.

2.2 Information security events, weaknesses and personal data breaches are reported to the Directors in line with this procedure.

2.3 The Directors are responsible for managing information security events, weaknesses and personal data breach responses

2.4 The Directors are responsible user training and awareness and for selecting those events which can be used to support training activities.

3. Information Security Breaches Procedure

3.1 Information security weaknesses and events are reported immediately after they are seen or experienced, on the Incident Management form, which can be obtained from the main office.

3.2 Users are not allowed to continue working after identifying a possible information security weakness, event or personal data breach.

3.3 The Directors will report back, by email, with a copy to the user's Manager, to describe how the event or breach was dealt with and closed out.

3.4 A copy of this e-mail is filed, together with the incident report, and any documentation arising from the event and the response to it that has been generated

4. Personal Data Breaches Procedure [Articles 33 & 34 of EU GDPR]

4.1 In the case of a personal data breach, the Directors determine whether it requires the relevant statutory notifications under the EU GDPR in accordance with GDPR Breach Notification Procedure

Signature: 

Date 30.06.24

INFORMATION SECURITY POLICY

Purpose

The Board of Directors and management of Blakeney Leigh Limited Limited, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with the Company's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

Our current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Business Continuity Plan and are supported by specific documented policies and procedures.

We aim to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the Company, the results of risk assessments and the risk treatment plan.

All Employees of Blakeney Leigh Limited Limited are expected to comply with this policy and with the ISMS that implements this policy. All Employees and certain external parties will receive appropriate training. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement and we are committed to achieving compliance with the GDPR.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

Signature:  Date 30.06.24

PASSWORD POLICY

1 Blakeney Leigh Limited controls access to information on the basis of business and security requirements.

2 Access control rules and rights to applications, expressed in standard user profiles, for each user / group of users are clearly stated, together with the business requirements met by the controls.

3 The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

4 The access rights to each application take into account:

- 4.1 Premises access control – unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems are located.
- 4.2 System access control – access to data processing systems is prevented from being used without authorisation.
- 4.3 Data access control – Persons entitled to use a data processing system gain access only to the data to which they have a right of access.
- 4.4 Personal data cannot be read, copied, modified or removed without authorisation.
- 4.5 The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements.
- 4.6 Data protection (EU GDPR) and privacy legislation and contractual commitments regarding access to data or services.
- 4.7 The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).
- 4.8 'Everything is generally forbidden unless expressly permitted'.
- 4.9 Rules that must always be enforced and those that are only guidelines
- 4.10 Prohibit user initiated changes to information classification labels
- 4.11 Prohibit user initiated changes to user permissions.
- 4.12 Enforcing rules that require specific permission before enactment.
- 4.13 Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

5 The Company has standard user access profiles for common roles

6 Management of access rights across the network(s) is by permission from the Directors only

7 User access requests, authorisation and administration are segregated

8 User access requests are subject to formal authorisation, to periodic review and to removal.

Signature:  Date 30.06.24

SUBJECT ACCESS REQUEST PROCEDURE

1. Scope

All personal data processed by Blakeney Leigh Limited is within the scope of this procedure.
Data subjects are entitled to obtain:

- Confirmation as to whether the Company is processing any personal data about that individual;
- Access to their personal data;
- Any related information;

2. Responsibilities

2.1 The Data Protection Officer John Ottley is responsible for the application and effective working of this procedure, and for reporting to the information owner on Subject Access Requests (SARs).

2.2 The Data Protection Officer is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests are made using the Subject Access Request Record

3.2 The data subject provides the Company with evidence of their identity, in the form of current passport / driving license and the signature on the identity must be cross-checked to that on the application form

3.3 The data subject specifies to the Company specific set of data held by the Company on their subject access request (SAR). The data subject can request all data held on them.

3.4 The Company records the date that the identification checks were conducted and the specification of the data sought.

3.5 Blakeney Leig Limited provides the requested information to the data subject within one month from this recorded date.

3.6 Once received, the subject access request (SAR) application is immediately forwarded to the Data Protection Officer who will ensure that the requested data is collected within the specified time frame in clause 3.4 above.
Collection entails:

3.6.1 Collecting the data specified by the data subject, or

3.6.2 Searching all databases and all relevant filing systems (manual files) in the Company, including all back up and archived files (computerised or manual) and all email folders and archives

3.7 The Data Protection Officer maintains a record of requests for data and of its receipt

3.8 The Data Protection Officer reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.9 If any of the requested data is being held or processed under one of the following exemptions, it does not have to be provided:

- National security
- Health
- Education
- Publicly available information

- Management forecasts
- Self-incrimination

3.10 In the event that a data subject requests the Company to provide them with the personal data stored by the controller/processor, then the Company will provide the data subject with the requested information in electronic format, unless otherwise specified.

3.11 In the event that a data subject requests what personal data is being processed then the Company provides the data subject with the following information:

3.11.1 Purpose of the processing

3.11.2 Categories of personal data

3.11.3 Recipient(s) of the information, including recipients in third countries or international organisations

3.11.4 How long the personal data will be stored

3.11.5 The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.

3.11.5.1 The Company removes personal data from systems and processing operations as soon as the data subject has submitted a request for erasure.

3.11.5.2 The Company contacts and communicates with other organisations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.

3.11.5.3 The Company takes appropriate measures without undue delay in the event that the data subject has: withdrawn consent; objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.

3.11.6 Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so

3.11.7 Information on the source of the personal data if it hasn't been collected from the data subject.

3.11.8 Inform the data subject of any automated decision-making.

3.11.9 If and where personal data has been transferred and information on any safeguards in place.

Signature:  Date 30.06.24

USER IDENTITY AND ACCESS MANAGEMENT POLICY

1. Scope

The access rights of all users/user groups to any of Blakeney Leigh Ltd's information assets, systems or services are managed in accordance with this procedure. The Company operates a single sign-on process as detailed in the Password Policy

2. Responsibilities

2.1 The Head of IT (CIO), John Ottley is responsible for administration of allocated and authorised user/user group access rights in conformity with the policy.
2.2 The Directors are responsible for initiation and administration of new and changed user access requests (user agreements) and user training.
2.3 The Directors are responsible for authorising access requests as being in line with business and organisational security policy and procedure.
2.4 Asset owners are responsible for authorising access requests to their information assets as being in conformity to the security requirements of the asset.
2.5 The Information Security Manager, John Ottley is responsible for reviewing user access rights in line with the review requirements of the GDPR.

3. User registration and de-registration

3.1 User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access.
3.2 Every user's proposed access rights are documented in a User Agreement, which details the systems/services/applications/information assets to which access is to be granted, together with the level of access that is to granted, taking into account the Password Policy. If a user is to be granted access rights then the specific additional authorisation of the Information Security Manager is also required.
3.3 The Directors and the system/asset owner authorise access to the system/asset.
3.4 The User Agreement is then signed by the user and passed to the Head of IT (CIO) and the username/user ID is created and administered.
3.5 The IT Department maintains a list of authorised users, administers changes in access rights and removes users.
3.6 The disciplinary policy will be invoked in cases of attempted unauthorised access.

4. Privilege management

4.1 Privileges are allocated to a different username than that allocated for normal use.
4.2 The available access privileges for each of The Company's operating systems, applications and other systems,
4.3 Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated in an e-mail from the user concerned to the Information Security Manager, which sets out the reasons why the privilege is required and the duration for which it is required.
4.4 The Information Security Manager retains a log of all privileges authorised and allocated and checks on a regular basis that they have been de-activated as specified in the original request.
4.5 The Information Security Manager checks that unauthorised privileges have not been obtained.

5. Password management

5.1 The allocation of passwords is formally controlled.
5.2 User password responsibilities are documented in their signed User Agreements
5.3 Users are initially issued with a unique temporary password, which they are forced to change at first logon.
5.4 Password changes are enforced, re-use of passwords is prohibited for 16 subsequent attempts, and seven-character alphanumeric passwords are required.
5.5 Users who need to be issued with a replacement password must first obtain the written authorisation of their Manager (who is required to confirm the identity of the user); this written authorisation must be presented to the Directors before a new unique temporary password can be issued.
5.6 Passwords are stored separately from application system data
5.7 The default passwords on all new equipment are changed to conform to the Company's password requirements before the equipment is brought into service.

6. Review of user access rights

6.1 Access rights are reviewed regularly and their adequacy is confirmed; any changes that need to take place are actioned.
6.2 User access rights are reviewed when a user's role or location within the Company changes in any way. If the access rights need to change, a new user agreement is issued, in line with this procedure, setting out those access rights.

Signature:  Date 30.06.24

DATA PROTECTION POLICY

Data Protection Policy

Purpose

This policy is designed to clarify and provide guidance on the Data Protection Act. A summary of areas covered by this policy is detailed below. Should you have any questions in relation to this document please speak to your Line Manager:

- General principles of the Policy
- Definition of Personal data
- Responsibilities with regards to data protection
- Processing and Access to Personal Data
- Employee Personal and Sensitive Information
- Transmitting and Monitoring

General Principles

It is the Company's approach that personal information is:

- Used fairly and lawfully
- Used for limited specifically stated purposes
- Used in a way that is adequate, relevant and not excessive
- Accurate
- Kept for no longer than is absolutely necessary
- Kept safe and secure
- Not transferred outside the UK without adequate protection

This is in line with the Data Protection Act 1998 and the principles contained within the Act.

Background

During the course of employment with the company employees may come into contact with and use confidential personal information about people, such as names and addresses or even information about customers' circumstances, families, health and other private matters.

Staff processing personal data on behalf of the Company have a responsibility to treat such data in line with the Data Protection Act and as directed by the Company (the Data Controller). The Company will comply with its obligations under the Data Protection Act.

The rules in this policy apply to all employees.

Definition of Personal Data

Personal data is information about a living person who can be identified by that information, or by other information which is in the possession of the Company. Information includes any expression of opinion about the individual, and any indication of the intentions of the Company, or another person about the individual.

Whether the information is on paper, video tape, computer, cassette, the Data Protection Act applies.

Processing Personal Data

"Processing" personal data includes obtaining, recording, organising, adapting, altering, retrieving, consulting, using, holding, disclosing, publishing, aligning, combining, blocking, erasing or destroying personal data.

The Data Protection Act 1998 provides strict rules in the relation to processing such personal data about data subjects. If employees are in any doubt about what they may or may not do, they should seek advice from their manager. If employees are in doubt and cannot get in touch with their manager or the Company Data protection Officer, the information concerned should not be disclosed.

The Company also holds and processes personal data about its employees. In the employment contract employees have consented to the data being used as set out in the contract. If this personal data changes employees should inform the Company in order that records can be updated.

Staff processing personal data on behalf of the Company have a responsibility to treat such data in line with the Data Protection Act and as directed by the Company (the Data Controller).

Access to Personal Data

Employees and others (Data subjects) may request to inspect personal information which the Company holds in relation to them and request that any inaccuracies are corrected. Requests should be made in writing to the Data Protection Officer and a fee may be charged for this service in line with the Data Protection Act. This fee amount will be confirmed prior to allowing access to the information.

Employee Personal Information

It is important that employees immediately notify any changes in personal information to their manager. These include changes to personal data as part of employment which generally covers the following:

- Change of name
- Change of address and telephone number
- Change to dependants (e.g. for parental and emergency leave requests)
- Change of name and contact details of next of kin and persons to be notified in case of emergency if different
- Change in professional and educational qualifications (for validation and legislation)
- Changes to tax code and National Insurance number (for payroll purposes)
- Changes to bank account (for Salary payment)
- Changes to driving license (where relevant to the employees role/claims)
- Evidence of entitlement to work in the UK
- Change to nominated beneficiaries (relates to Death in Service Policy or Pensions Policy

Sensitive Personal Information

The Company may also hold sensitive personal information, including of the following kind, any changes to which (as appropriate) must be notified to the manager immediately:

- Racial or ethnic origins (focused on equal opportunity monitoring)
- Religious beliefs or similar (focused on equal opportunity monitoring and medical needs)
- Trade union membership (focused on union administration purposes)

- Physical or mental health (focused on SSP, SMP, equal opportunities monitoring and employment administration purposes)
- Commission (or alleged commission) of an offence (focused upon detection of misconduct and employment administration purposes)

The Company will ensure that sensitive information is securely held and properly administered in accordance with the Act.

It is important that changes in personal circumstances (including the above personal and sensitive data) are notified to the manager immediately.

Transmitting Information

All employees should be aware of the risks when transmitting personal data. The following is guidance for employees responsible for personal data:

- Pay particular attention to the risks of transmitting confidential employee information by email or fax
- Transmit information between locations only if a secure network or comparable arrangements are in place or if, in the case of email, encryption is used
- All copies of email and fax messages received by managers should be held securely
- The Company draws your attention to the risks of sending confidential, personal information by email or fax

If the Company sells all or part of its business it may provide personal data about employees to any prospective purchaser in the course of negotiations. So far as possible such data will be provided in an anonymous form and if this is not possible the prospective purchaser will be required to keep the information confidential. We will transfer any personal data on any transfer or sale falling within the terms of the Transfer of Undertakings (Protection of Employment) Regulations.

Monitoring

The Company monitors emails and telephone calls but strictly in accordance with what is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Employees have consented to this by a term in the employment contract.

Any data protection queries should be addressed to a Director.

Further Information

The Company will review policies and procedures periodically to reflect changes in legislation, good practice etc.

Signature:  Date 30.06.24

Business Continuity Plan

Maintaining this document is the responsibility of: John Ottley

This document will next be reviewed: June 2024

The following premises are covered in this document:
3 Sherman Walk
Greenwich
London
SE10 0YJ

Copies of this document can be found:
John Ottley Laptop/Blakeneyeigh/Policies/BCP
BLShare/Practicebusiness/Officepolicies/BCP

Contents

Recommended Maintenance

Items which may need to be updated regularly include:

- *Team members*
- *Managers' responsibilities*
- *Applications (new or significant changes to existing)*
- *Insurance provider and contact details*
- *Internet / telephone provider and contact details*
- *Staff contact details*

The next review of this document is detailed on the front cover or shall be carried out following enactment following an incident or test review.

Business Continuity Overview

Purpose

The purpose of this plan is to prepare our business in the event of extended service outages caused by factors beyond our control and to restore services to the widest extent possible in a minimum time frame.

Outcome

The outcome of this plan is to ensure that the business is able to maintain a good level of service for our customers

Plan objectives

- Serves as a guide for those implementing our business continuity plan
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
-

Key staff

If a disaster occurs the members of our team tasked with enacting this plan are:

John Ottley	(Managing Director)	+44 7811 266520	john.ottley@blakeneyleigh.co.uk
Neal Gordon	(Director)	+44 7813 210533	neal.gordon@blakeneyleigh.co.uk
Neil Redman	(IT)	+44 7973 294965	neil@santikara.co.uk

Staff Welfare

It must be recognised that an incident that results in the enacting of this plan may also cause additional pressures for staff. Staff members need to be given clear direction about the priorities of the business. Directors must ensure that they monitor staff more closely to ensure that their welfare is maintained.

Staff should be aware of what their role is when a major disruption occurs. Clear and concise communication with staff is pivotal to having an organised response. Staff must be made aware of what communication methods are going to be used so they can find out the latest information, if they are going to be working from a different location than normal.

Directors who suspect that staff members have suffered undue stress or even trauma from the business disruption must consider the provision of assistance for those staff who have been affected.

Communicating with staff

John Ottley shall contact the first staff member to confirm the issue and time frame of actions to be taken, information shall be propagated as the table below.

Client shall be informed of the cause of disruption and the level of expected disruption to our services, together with a time frame for rectification and reinstatement of service level.

Primary communication shall be by mobile phone with follow up email, Blakeney Leigh also have an internal whats app group.

All staff contacts are detailed in this document as well as being recorded on handheld mobiles, contacts are also stored on cloud servers so are available at all times.

Staff should not discuss any with the media, this shall be coordinated through Neal Gordon to represent the business.

Any event that disrupts the provision of service to a client shall be notified to that client.

Staff Cascade System

Staff Member	Point of Contact
John Ottley	Neal Gordon Stuart Smith Leigh Ives
Stuart Smith	Sam Geoghegan Jan Martin Laura Dimitru
Sam Geoghegan	Chris Orford Joe Aylward Harry Miller
Chris Orford	Maria Wade Alex Draper Jess Kirby
Alex Draper	John Ottley Rob Wellard Michael MacDonald

Equipment

Most staff have their own laptops and i-pads provided by Blakeney Leigh and as such these are unlikely to be directly affected by the disaster affecting the office-based equipment, where laptops are affected these will be replaced to allow continuity of working from outside the office.

Office based staff do not have access to laptops as they are insufficiently powerful to run the specialist software (Revit) their replacement however is available directly off the shelf and the software can be readily downloaded to allow operation to be commenced within 2 days.

All lap tops are provided with alternate email addresses by an alternate provider, these are also mirrored to ipads issued to each surveyor.

Replacement equipment will be purchased and distributed by John Ottley or Neal Gordon where necessary, replacement equipment is available off the shelf direct from local retailers.

All staff have a smart-phones which will can provide email and telecommunication contact between staff and customers, emails are hosted so outside the direct control of Blakeney Leigh

Staff Member	Contact number	Email address	Alternate email address	Laptop	ipad
John Ottley	07811266520	john.ottley@blakeneyleigh.co.uk	jottley@icloud.com	Issued	personal
Neal Gordon	07813210533	neal.gordon@blakeneyleigh.co.uk	ngordon@1cloud.com	Issued	personal
Stuart Smith	07920228169	stuart.smith@blakeneyleigh.co.uk	Blakeneyleigh1@icloud.com	Issued	Issued
Leigh Ives	07854950752	leigh.ives@blakeneyleigh.co.uk	Blakeneyleigh2@icloud.com	Issued	Issued
Sam Geoghegan	07391418894	sam.geoghegan@blakeneyleigh.co.uk	Blakeneyleigh.6@icloud.com	Issued	Issued
Chris Orford	07391418894	chris.orford@blakeneyleigh.co.uk	Blakeneyleigh.8@icloud.com	Issued	Issued
Leigh Ives	07854950752	Leigh.ives@blakeneyleigh.co.uk	Blakeneyleigh.3@icloud.com	Issued	Issued
Rob Wellard	07985360278	rob.wellard@blakeneyleigh.co.uk	Blakeneyleigh.4@icloud.com	Issued	Issued
Harry Miller	07584832912	harry.miller@blakeneyleigh.co.uk	N/A	Issued	Issued
Alex Draper	07564421921	alex.draper@blakeneyleigh.co.uk	Blakeneyleigh.9@icloud.com	Issued	no
Laura Dimitru	07538292823	Laura.dimitru@blakeneyleigh.co.uk	N/A	No	no
Joe Aylward	07921225538	Jo.Aylward@blakeneyleigh.co.uk	N/A	No	no
Michael MacDonald	07749497297	Michael.macdonald@blakeneyleigh.co.uk	N/A	No	no
Maria Wade	02087777700	maria.wade@blakeneyleigh.co.uk	N/A	No	no
Jan Martin	02087777700	jan.martin@blakeneyleigh.co.uk	N/A	No	no
Jess Kirby	07826044187	Jess.kirby@blakeneyleigh.co.uk	N/A	Issued	Issued
Neil Redman	07973294965	neilr@santikara.co.uk	N/A	External consultant	External Consultant

Blakeney Leigh has a RAID data server that is mirrored to minimise the risk of failure, this system is backed up and stored off site.

Neil Redman (IT) will be responsible for uploading the off-site data back to the server

Blakeney Leigh has a separate email server providing email connection and email storage placing less reliance on the main server, all emails are stored off site by our internet provider.

Software	Licence Key	Password	Users
Autodesk	568-08164497	Via email	Laura Dimitru
Microsoft Office	H6TY7-V9VHJ-FQ7X2-X7F9H-BPKD4 P7XPQ=GR76J-XBYTY-W92B3-RYV7C TDBC3-794HV-Y8W48-69QRV-WG92V 4CGG4-3KJYC-MVGD9-Y3V43-JY9HK P34T4-MPHKK-XBMRP-TWXHD-TPY4G TB3FM-JGHXM-HR3RP-FGBV3-Q34TD JW34R-MMN68-JHHHJ-HMX4P-XTJ7R PBQH6-N6YFF-KJFY7-DCT6J-GVGHR BDY7N-8PMMB-T8QBP-FWK2D-C37PX	Not disclosed	John Ottley Neal Gordon Stuart Smith Leigh Ives Sam Geoghegan Chris Orford Maria Wade Jan Martin Alex Draper Rob Wellard Harry Miller Michael MacDonald Lura Dimitru Joe Aylward
Adobe	Creative cloud licence	Via email	John Ottley
Sage	Cloud account	Via email	Steve Broughton John Ottley Maria Wade
Bank Account	On line account	Not disclosed	Steve Broughton John Ottley Maria Wade Clare smith

Critical Software has been purchased online and requires activation following download or through an account activation.

Accounts, Pay Role and Banking are all provided with cloud access and as such our accounts are protected from a disruptive event at Blakeney Leigh, all accounts are backed up from the cloud and stored off site

Up front cost would be expected to be minimal circa £15,000.00 in the initial phase and basic services should be up and running within 2 days with full service being available within 5 days.

Scenario 1

Premises incident

A premises incident can include flood, fire, or any other disaster that renders our office inaccessible.

Step 1: Evacuation of premises & safeguarding of staff

In office hours

Action	Details	Responsible Person(s)
1. Evacuate the building	Follow normal fire drill procedure	John Ottley Director
2. Check evacuation is complete	Staff and visitor safety is the priority. Check everyone on-site has been evacuated	John Ottley Director
3. Verify if incident is real	If false alarm, resume business as normal	John Ottley Director
4. Call emergency services	999	John Ottley Director
5. Record details of any injuries sustained in the incident	Use injury form available on internet	John Ottley Director
6. Alert staff	Alert any staff due to arrive on-site soon of the incident, and tell them to await further instructions	John Ottley Director
7. Assess impact	Senior team meet to assess the scale of the incident & decide next steps	John Ottley Director

Outside office hours

Action	Details	Responsible Person(s)
1. First person on-site to notify manager	Do not enter the building	All staff
2. Call emergency services	999	All staff
3. Alert staff	Alert any staff due to arrive on-site soon of the incident, and tell them to await further instructions	All staff
4. Assess impact	Senior team meet to assess the scale of the incident & decide next steps	John Ottley Director

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
Phones	Staff to use personal mobile phones. Contact telephone provider to forward office line to staff mobiles 4Comm Tel:0330 444 4444	John Ottley Director
Internet	Staff to use home internet connections. If home connection unavailable contact local shared office providers to rent desk space	John Ottley Director
Inform insurance company	David Gauntlett Nex Gen Insurance Tel:01732 496 000	Neal Gordon Director
Inform landlord	River Gardens Tel:020 3372 2641	Neal Gordon Director
Post redirection	Form available from Royal Mail	Neal Gordon Director
Inform customers	If disruption is expected, inform customers via email and telephone	Maria Wade

Scenario 2

Infrastructure incident

An infrastructure incident can include the loss of computer / telephony systems, internet access, or power.

Step 1: Understand the extent of the loss

Infrastructure	Details	Responsible Person(s)
Phones	Contact phone provider to ascertain extent of outage. Contact details: 4Comm Tel:0330 444 4444	Neal Gordon Director
Internet/Email	Contact internet provider to ascertain extent of outage. Contact details: ZEN Internet Limited Tel: 01706-902-000	Neal Gordon Director Neil Redman IT
Mains power	Contact power provider to ascertain extent of outage. Contact details: BES Tel:03445 678 427	Neal Gordon Director

If outage is temporary, inform staff to stay put and await further instructions. If the outage is ongoing:

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
Phones	Staff to use company mobile phones. Contact telephone provider to forward office lines to staff mobiles 4Comm Tel:0330 444 4444	Neal Gordon Director
Internet	Staff to use home internet connections. If home connection unavailable contact Cignia to arrange shared office facility 020 3714 5640	Neal Gordon Director
Mains power	Staff to work from home until power is restored. If power outage is widespread and staff homes are also	Neal Gordon Director

	affected contact Cignia to arrange shared office facility. 020 3714 5640	
Email	Alternate email address to be circulated to customers, apple email address already secured for ipad usage.	John Director Ottley

Scenario 3

Staff incident

A staff incident can include a sudden family emergency, injury or other event which renders a key member of staff suddenly unable to work.

Step 1: Ensure no service interruption

Critical activity	Details	Responsible Person(s)
1. Identify interchangeable staff	All members of staff have team members who can perform their roles, even if it is in a reduced capacity. Identify the relevant person and support them in carrying out business-critical activities	John Ottley Director
2. Assess extent of loss	Identify whether the affected staff member's absence is likely to be temporary, longer-term, or permanent. Keep in mind this may be a difficult period for the staff member and / or their family.	John Ottley Director

If the staff loss is temporary, support the member of staff who will be filling the gap until the absent member of staff returns. If the absence is long-term or permanent. Staff are not pre-allocated to cover individuals as this is on a job specific basis as a contract or commission is awarded by the client, At award a main point of contact is provided and Blakeney Leigh allocate an individual to provide cover if required.

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
1. Recruit temporary or full-time replacement	Follow the standard recruitment procedure to find a full-time, part-time or fixed-term contract (as appropriate) replacement.	John Ottley Director

Blakeney Leigh has a relationship with Hays recruitment and receive a number of CV's on a regular basis to allow awareness of the employment market and have an up to date selection of applicants to review.

Recovery phase

The purpose of the recovery phase is to resume normal working practises for the entire organisation. Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building.

Action	Details	Responsible Person(s)
1. Agree and plan the actions required to enable recovery of normal working practises	Agreed actions will be detailed in an action plan and set against time scales with responsibility for completion clearly indicated.	John Ottley Director Neal Gordon Director
2. Respond to any long term support needs of staff	Depending on the nature of the incident, we may need to consider providing support services	John Ottley Director
3. Publicise that there is now 'business as usual'	Inform customers through normal channels that our business is operating as normal	Neal Gordon Director
4. Carry out a debrief of the incident and complete report to document opportunities for improvement and any lessons identified	This should be reviewed to ensure key actions resulting from the incident are implemented within designated time scales.	Neal Gordon Director
5. Review this Continuity Plan in light of lessons learned from incident and the response to it	Implement recommendations for improvement and update this plan. Ensure a revised version of the plan is read by all members of staff.	John Ottley Director

Signed by Director

John Ottley

30.06.24