Data Protection Policy

Suzanne Barnes Design Partnership Ltd

Contents

Prepared by:	Suzanne Barnes
Approved by The Directors on:	31st May 2023
Valid from:31st May 2023	

1 Introduction

1.1 We, Suzanne Barnes Design Partnership Ltd obtain, use and retain personal information as part of our day-to-day activities and for various specific lawful purposes such as invoicing and sharing with known contractors and suppliers. That personal data relates to current, former and prospective clients, directors, employees, interns, contractors, agency workers, volunteers, trainees and apprentices, suppliers and third parties. In doing so, we are subject to various legislative provisions including those set out in the United Kingdom General Data Protection Regulation (**UK GDPR**), the Data Protection Act 2018 (**DPA18**) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**PECR**). We are also subject to the EU General Data Protection Regulation (**EU GDPR**) in relation to goods and services we offer to individuals and our wider operations in the European Economic Area (**EEA**).**]** These legislative provisions address how we, as data controllers and data processors, should obtain, deal with and retain personal data and we are committed to complying with those provisions and to being concise, clear and transparent in how we obtain, use and delete (where relevant) that personal data.

1.2 We are registered with the Information Commissioners Office (**ICO**)

1.3 The purpose of this policy is to set out the means by which we comply with those data protection obligations and the means by which we protect personal information relating to data subjects. This includes our obligations as to the collection, processing, transfer, storage, and disposal of that personal data.

1.4 Suzanne Barnes has been appointed as our data protection manager. They are responsible for informing and advising us on our data protection obligations, for monitoring compliance and for ensuring that we comply with our obligations in accordance with our policies. Comments or queries concerning this policy should be addressed to them.

1.5 The data protection manager will deal with issues relating to this policy and the application of data protection law including:

1.5.1 issues relating to the correct lawful basis to be applied to personal data collected, held or processed and in particular when consent or legitimate interest is being relied upon;

1.5.2 issues relating to the use to which data can be put having regard to the purpose for which it was acquired;

1.5.3 issues relating to the periods for which personal data is retained;

1.5.4 privacy notices and when these are required;

1.5.5 subject access requests and other data subject rights as set out in Articles 12 to 23 of the UK/EU GDPR;

1.5.6 actual or suspected data breaches or issues relating to security arrangements;

1.5.7 sharing data with third parties and transferring data outside the UK and EEA

1.5.8 where processing uses new technologies and is likely to result in a high risk to the rights and freedoms of natural persons and a data protection impact assessment is required;

1.5.9 in relation to automated processing, including profiling or automated decision-making; and

1.5.10 in relation to information which is deemed to be special category data or data relating to children or criminal convictions.

2 Definitions

2.1 The definitions set out in Article 4 of the UK/EU GDPR shall apply to the terms used in this policy and in relation to data protection generally within this organisation.

2.2 Other definitions are set out in brackets throughout this policy.

3 Scope of this policy

3.1 This policy applies to the personal data of all of those referred to in paragraph 1.1 above.

3.2 This policy is intended to set out:

3.2.1 how data is protected;

3.2.2 how we comply with our data protection obligations;

3.2.3 what we will expect to be done by our directors, employees, contractors, agency workers, interns, volunteers and trainees in that regard.

It is intended that this policy will help to ensure that personnel understand and are able to comply with the various data protection requirements to which they are subject in the course of their work.

3.3 We have produced various other policies dealing with other areas of data and security. These are: [*list other relevant policies*]. All personnel should be aware of, and comply with, these policies in addition to complying with the terms contained within this policy.

3.4 The provisions in this policy apply to all personal data whether it is on paper or stored electronically and whether it is in writing or stored as

verbal messages. It applies whether the personal data is stored on our network, on individual desktop or laptop computers, on mobile devices, phones or tablets, in paper files or in any other way.

3.5 This policy will be reviewed and updated regularly in order to ensure that we continue to act in accordance with our data protection obligations. Revised versions will be brought to the attention of all personnel as and when necessary.

4 Processing personal information

4.1 Article 5 of the UK/EU GDPR requires that personal data is processed in accordance with the data protection principles. Therefore, when processing personal data, we must ensure that we:

4.1.1 process personal information lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

4.1.2 only collect personal data for specified, explicit and legitimate purposes and not process that data in a way that is incompatible with those legitimate purposes ('purpose limitation');

4.1.3 only process the personal data that is adequate, relevant and necessary for the purpose ('data minimisation');

4.1.4 keep the personal data accurate and up to date and take all reasonable steps to delete or correct inaccurate personal data without delay ('accuracy');

4.1.5 keep personal data in a way that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed subject to certain exceptions ('storage limitation'); and

4.1.6 process the personal data in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4.2 In addition to only processing data in accordance with the data protection principles, Article 6 of the UK/EU GDPR requires that we must also ensure that personal data is processed lawfully and in such a way that at least one of the following bases applies:

4.2.1 the data subject has given consent to the processing of his or her personal data for one or more specific purposes ('consent');

4.2.2 the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ('contract');

4.2.3 the processing is necessary for compliance with a legal obligation to which we are subject ('legal obligation');

4.2.4 the processing is necessary for the protection of the vital interests of the data subject or another natural person ('vital interest');

4.2.5 the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority ('public interest');

4.2.6 the processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child ('legitimate interest').

4.3 Where processing is based on consent, we must be able to demonstrate that the data subject has consented to the processing of his or her personal data and that such consent has been given in such circumstances that it is able to be clearly distinguishable from the other matters and in an intelligible and easily accessible form, using clear and plain language. The data subject shall have the right to withdraw his or her consent at any time which shall not, however, affect the lawfulness of processing based on consent before its withdrawal. When assessing whether consent is freely given regard must be had to the fact that the performance of a contract or provision of a service must not be made to be conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

4.4 Other than where the processing is based on consent, we must satisfy ourselves at all times that the processing is necessary for the purpose of the relevant lawful basis set out above and that there is no other reasonable way to achieve that purpose. In order to demonstrate compliance, we must document our decision as to which lawful basis applies and record information both concerning the purposes of the processing and the lawful basis relied upon. Where sensitive personal information or criminal offence information is to be processed, we must, in addition to the bases set out above, identify a lawful special condition for processing that information and document it.

4.5 Where we are relying upon legitimate interest as the appropriate basis for lawful processing, we must conduct a legitimate interest assessment (**LIA**) and keep a record of it, to ensure that we can justify our decision. In the event that the LIA identifies a significant privacy impact we must consider whether we also need to conduct a data protection impact assessment (**DPIA**).

4.6 If the personal data in question is special category personal data (**sensitive personal data**), then we can only process that data provided that we have a lawful basis for doing so as set out in paragraph 4.2 above, and at least one of the conditions set out below is met. Sensitive personal data is that which reveals 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. The conditions are:

4.6.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless UK domestic law or, where the EU GDPR prohibits them from doing so);

4.6.2 processing is necessary for the purposes of carrying out our obligations and exercising specific rights or those of the data subject in the field of employment and social security and social protection law in so far as it is authorised by UK domestic law or, where it applies, EU or EEA member state law or a collective agreement pursuant to UK domestic, EU or EEA member state law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

4.6.3 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

4.6.4 processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subjects;

4.6.5 the processing relates to personal data which is manifestly made public by the data subject;

4.6.6 the processing is necessary to establish, exercise or defend legal claims or whenever courts are acting in their judicial capacity;

4.6.7 the processing is necessary for substantial public interest reasons, on the basis of UK domestic law or, where the EU GDPR applies, EU or EEA member state law and it is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

4.6.8 the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of UK domestic law or, where the EU GDPR applies, EU or EEA member state law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9(3) of the UK/EU GDPR;

4.6.9 the processing is necessary for public interest reasons in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of UK domestic law or, where the EU GDPR applies, EU or EEA member state law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject and in particular, professional secrecy;

4.6.10 the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1)

of the UK/EU GDPR based on UK domestic law or, where the EU GDPR applies, EU or EEA member state law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4.7 If the personal data is sensitive personal data then the data protection manager must be notified, before processing commences, of the proposed processing so that they may assess whether the processing complies with the criteria set out above. No processing will commence until that assessment has taken place and the data subject has been informed and no automated decision-making (including profiling) will be based on any data subject's sensitive personal information.

4.8 Criminal records information will only be processed in accordance with our criminal records information policy.

5 Data protection impact assessments

5.1 Article 25 of the UK/EU GDPR requires that privacy by design principles be applied to all new projects or uses of personal data especially where they involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

5.2 A data protection impact assessment (**DPIA**) shall in particular be required in the case of:

5.2.1 a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

5.2.2 processing on a large scale of special categories of data referred to in Article 9(1) of the UK/EU GDPR, or of personal data relating to criminal convictions and offences referred to in Article 10 of the UK/EU GDPR; or

5.2.3 a systematic monitoring of a publicly accessible area on a large scale.

5.3 In such circumstances we will carry out a DPIA to assess:

5.3.1 the purposes of the processing, including, where applicable, the legitimate interest we are pursuing;

5.3.2 whether the processing is necessary and proportionate in relation to its purpose;

5.3.3 the risks to data subjects; and

5.3.4 the measures that can be put in place in order to address those risks and protect personal information.

5.4 In doing so, regard will be had to:

5.4.1 the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

5.4.2 the state of the art of all relevant technical and organisational measures to be taken;

5.4.3 the cost of implementing such measures; and

5.4.4 the risks posed to data subjects and this organisation, including their likelihood and severity.

5.5 The DPIA will be overseen by the data protection manager and shall address:

5.5.1 the type of personal data collected, held and processed;

5.5.2 why and how personal data is to be used;

5.5.3 our objectives;

5.5.4 who is to be consulted;

5.5.5 the necessity and proportionality of the data processing;

5.5.6 the risks to data subjects and to us; and

5.5.7 the measures taken to minimise and deal with those risks identified.

6 Documentation and record keeping

6.1 We will keep internal written records of those processing activities which we undertake in our role as data controller. In all cases those records will contain:

6.1.1 the name and contact details of the data protection manager and, where applicable, any joint controller, that controller's representative and their data protection manager;

6.1.2 the purposes of the processing;

6.1.3 a description of the categories of data subjects and of the categories of personal data;

6.1.4 the categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organisations;

6.1.5 where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in Article 49(1)(b), the documentation of suitable safeguards;

6.1.6 where possible, the envisaged time limits for erasure of the different categories of data;

6.1.7 where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

6.2 We will keep internal written records of those processing activities which we undertake in the role of data processor and shall maintain a

record of all categories of processing activities carried out on behalf of a controller, containing:

6.2.1 the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection manager;

6.2.2 the categories of processing carried out on behalf of each controller;

6.2.3 where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in Article 49(1)(b), the documentation of suitable safeguards;

6.2.4 where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

6.3 As part of our record of processing activities we will document:

6.3.1 information required for privacy notices;

6.3.2 records of consent;

6.3.3 controller-processor contracts;

6.3.4 the location of personal information;

6.3.5 DPIAs; and

6.3.6 records of data breaches.

6.4 In the event that we process sensitive personal information, we will keep written records of:

6.4.1 the purposes of the processing, including where relevant why it is necessary for that purpose;

6.4.2 the lawful basis for our processing; and

6.4.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

6.5 Regular reviews of the personal information we process will be undertaken and we will, where necessary, update our documentation accordingly.

7 Information provided to, and the rights of, data subjects

7.1 We will provide all data subjects with the information set out in paragraph 7.2 below. This will take place at the time of collecting the data where that data is obtained directly from the data subject or, where the data is obtained from a third party:

7.1.1 when the first communication is made if the personal data is used to communicate with the data subject;

7.1.2 before a transfer is made where the personal data is to be transferred to another party;

7.1.3 in all other cases, as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

7.2 The following information shall be supplied:

7.2.1 our details including contact details and the names and details of our data protection manager.

7.2.2 the purposes for which the personal data is being collected, how it will be processed and the lawful basis for that collection and processing;

7.2.3 any legitimate interests justifying its collection and processing;

7.2.4 where we have not obtained the personal data directly from the data subject, the categories of personal data collected and processed;

7.2.5 where we plan to transfer the personal data to one or more third parties, details of those parties;

7.2.6 where the transferee of the personal data is located outside the UK, details of that transfer, including any safeguards in place;

7.2.7 any relevant data retention periods;

7.2.8 the data subject's rights under the UK/EU GDPR.

7.2.9 the data subject's right to withdraw their consent to our processing their personal data.

7.2.10 the data subject's right to complain to the Information Commissioner's Office.

7.2.11 where we have not obtained the personal data directly from the data subject, details about the source of that personal data.

7.2.12 where relevant, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

7.2.13 any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

7.3 We will issue privacy notices from time to time, informing data subjects as to the personal information collected about them, how it is held and how they can expect that personal information to be used and for what purposes.

7.4 Any information provided in privacy notices will be in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

7.5 We will ensure that data subjects are informed that they have the following rights in relation to their personal data:

7.5.1 to be informed about how, why and on what basis their data is processed.

7.5.2 to obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request.

7.5.3 to have data corrected if it is inaccurate or incomplete.

7.5.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing.

7.5.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but they do not want the data to be erased), or where the personal information is no longer needed but it is required to be retained to establish, exercise or defend a legal claim.

7.5.6 to restrict the processing of personal information temporarily where they do not think it is accurate or where they have objected to the processing, and we are considering whether our legitimate aims override their interests.

7.5.7 to receive the personal data concerning him or her, which he or she has provided to us, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance from us, where the processing is based on consent pursuant to Article 6(1)(a) or Article 9(2)(a) or on a contract pursuant to Article 6(1)(b) and the processing is carried out by automated means.

7.6 A data subject may make a subject access request (**SAR**) at any time in order to find out more about the personal data which we hold about them, the processing we are carrying out and the purpose of that processing. We must normally respond to a SAR within one month of receipt. This may, however, be extended by up to two months if the SAR is complex and/or numerous requests are made but the data subject must be informed if we are to rely on this. All SARs received must be dealt with by the data protection manager. We do not charge a fee for dealing with a SAR in normal circumstances although we may charge a reasonable fee for further copies of information already provided or for requests that are manifestly unfounded or excessive, particularly where those requests are repetitive.

7.7 A data subject has the right to require us to rectify any personal data that is inaccurate or incomplete. We must do so within one month of the data subject informing us and we must inform the data subject that we have done so. We can extend this period by up to two months where the requests are complex, but the data subject must be informed if we are to rely on this. If the personal data in question has been sent

to third parties, those third parties should wherever possible be informed of the rectification.

7.8 The data subject has the right to request that we erase the personal data we hold about them in the following circumstances:

7.8.1 where it is no longer necessary for us to retain that personal data having regard to the purpose for which it was originally collected or processed.

7.8.2 where the data subject wishes to withdraw consent to holding and processing personal data previously given to us.

7.8.3 where the data subject objects to us holding and processing their personal data and no overriding legitimate interest permitting us to continue doing so exists.

7.8.4 the personal data has been processed unlawfully.

Unless we have reasonable grounds for refusing to erase personal data, all erasure requests shall be complied with within one month from the receipt of the data subject's request. The data subject must be informed. We can extend this period by up to two months where the requests are complex, but the data subject must be informed if we are to rely on this. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties are to be informed of the erasure unless to do so is impossible or would require disproportionate effort.

7.9 A data subject may request that we cease processing their personal data in which case we may retain only that personal data that is necessary to ensure that the data subject's personal data in question is not processed further. In the event that this data has been disclosed to third parties, those parties are to be informed of the processing restriction unless to do so is impossible or would require disproportionate effort.

8 Confidentiality and information security

8.1 All personnel must keep confidential data about all data subjects for which they are responsible or to which they have access. Failure to do so would be a breach of our duties under the UK/EU GDPR, DPA18 and any professional or similar regulations to which we are subject.

8.2 Personnel who have access to personal data must:

8.2.1 only access the personal data which they have authority to access, and only for authorised purposes.

8.2.2 only allow other personnel to access personal data if they have appropriate authorisation.

8.2.3 only allow individuals who are not members of our staff to access personal data if specific authority to do so exists.

8.2.4 keep personal data secure, for example by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in our information security policy.

8.2.5 whenever passwords are used to protect personal data. **We must review our passwords regularly**. All personnel must abide by our password policy

8.2.6 not remove personal data, or devices containing personal data (or which can be used to access it), from our premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the data and the device and they have authority to do so;

8.2.7 ensure that if personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, that the computer and screen are locked before the user leaves it.

8.2.8 not store their own personal information on local drives or on personal devices that are used for work purposes or store work-related information on local drives or on personal devices that are used for personal purposes and comply in **all respects with our Bring Your Own Device policy.**

8.3 In the event that any personnel have any concerns or suspicions that any of the matters set out below are taking place, they should immediately inform the data protection manager of those concerns or suspicions:

8.3.1 personal data is being processed without a lawful basis or, in the case of sensitive personal information, without one of the conditions in paragraph 4.6 above being met;

8.3.2 a data breach;

8.3.3 personal data is being accessed without the proper authorisation;

8.3.4 personal data is not being retained or deleted securely;

8.3.5 personal data, or devices containing personal data, are being removed from our premises without appropriate security measures being in place;

8.3.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

8.4 We will use all appropriate technical and organisational measures in order to keep personal data secure and to protect it from unauthorised or unlawful processing and accidental loss, destruction or damage. Those measures may include:

8.4.1 ensuring that wherever possible personal data is pseudonymised or encrypted;

8.4.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

8.4.3 ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

8.4.4 the regular testing, assessing and evaluating of effectiveness of technical and organisational measures for ensuring the security of the processing.

8.5 In the event that we use external organisations to process personal data on our behalf, we will ensure that additional security arrangements are implemented in contracts with those organisations in order to safeguard the security of personal data. In particular, contracts with external organisations will provide that:

8.5.1 the external organisation may act only on our written instructions;

8.5.2 those processing the data are subject to a duty of confidentiality similar to that set out above;

8.5.3 appropriate measures are taken to ensure the security of processing;

8.5.4 sub-contractors are only engaged with our prior consent and only under a written contract;

8.5.5 the external organisation will assist us in providing subject access and allowing individuals to exercise their rights in relation to data protection;

8.5.6 the external organisation will assist us in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

8.5.7 the external organisation will delete or return all personal information to us as requested at the end of the contract; and

8.5.8 the external organisation will submit to audits and inspections, provide us with whatever information we need to ensure that they are meeting their data protection obligations; and

8.5.9 the external organisation will inform us immediately if it is asked to do something infringing data protection law.

8.6 No one may enter into an agreement with an external organisation to process personal data on our behalf without the consent of the data protection manager.

9 Storage and retention of personal information

9.1 We must not retain personal data (and in particular sensitive personal data) for any longer than necessary. The length of time over which data may be retained is dependent upon the circumstances including why the personal information was obtained in the first place.

9.2 We will ensure that the following measures are taken as to the storage of personal data:

9.2.1 All electronic copies of personal data will be stored securely using passwords and appropriate data encryption;

9.2.2 We will store securely all hardcopies of personal data. This will include electronic copies of data that are stored on physical or other removable media;

9.2.3 Suitable backups will be made of all personal data that is stored electronically. We will adopt the 3-2-1 method for backups, keeping at least three (3) copies of our data, store two (2) backup copies on different storage media and keep one (1) of them located offsite. All backups will be encrypted;

9.2.4 Personal data must not be stored on mobile devices (including memory sticks, laptops, tablets, and smartphones) without the consent of the data protection manager and, in the event that such approval is granted, for no longer than is absolutely necessary;

9.2.5 **Personal data will not be transferred to any device personally belonging to any member of personnel. Unless permission granted by the data protection manager**

9.3 We must delete permanently from our information systems any personal data (and sensitive personal data) that is no longer required and destroy any hard copies securely in accordance with our data retention policy.

10 Transferring personal data outside the UK [and EEA]

10.1 We currently do not need to transfer, make available remotely or store remotely personal data in or to countries outside the UK and EEA.

11 Data breaches

11.1 A data breach is any loss of data or information in whatever form it is held and by whatever means the data was lost including data that is destroyed or rendered unusable. It may take many different forms, including:

11.1.1 loss or theft of data or equipment on which personal information is stored;

11.1.2 unauthorised access to or use of personal information either by a member of staff or third party such as from hacking;

11.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

11.1.4 human error, such as accidental deletion or alteration of data;

11.1.5 unforeseen circumstances, such as a fire or flood;

11.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

11.1.7 social engineering such as phishing and vishing, where information is obtained by deception.

11.2 All personal data breaches must be reported immediately to the data protection manager.

11.3 In the event that any personnel become aware of a data breach, or suspect that a data breach has occurred, they must not attempt to investigate it themselves as this can lead to further issues arising. They

must instead report all evidence relating to the personal data breach to the data protection manager.

11.4 Where a personal data breach that is likely to result in a risk to the rights and freedoms of data subjects occurs, the data protection manager, must ensure that the Information Commissioner's Office (**ICO**) is informed of that breach without delay, and in any event, within 72 hours after having become aware of it.

11.5 Where a personal data breach may result in a high risk that the rights and freedoms of data subjects will be compromised, the data protection manager must ensure that all data subjects affected by that breach are notified directly and without undue delay.

11.6 A data breach notification shall at least:

11.6.1 describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

11.6.2 communicate the name and contact details of the data protection manager or other contact point where more information can be obtained;

11.6.3 describe the likely consequences of the personal data breach;

11.6.4 describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

12 Training

12.1 We will ensure that all personnel receive adequate training as to their data protection responsibilities and as to how to act and respond as and when they receive requests for matters such as subject access requests, objections and requests for erasure and rectification**. It is imperative that all personal record any suspicions or breaches that they may suspect.** Those whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

12.2 Information will be provided to all new personnel as part of their induction training.

13 Failure to comply

13.1 We regard compliance with this policy as an extremely serious matter. Failing to comply puts at risk those individuals whose personal information is being processed, carries the risk of significant civil, criminal and regulatory sanctions for us and our personnel and may, in some circumstances, amount to a criminal offence by the individual.

13.2 Because of the importance of this policy, any failure to comply with provisions set out in this policy by any personnel will be taken seriously and may lead to disciplinary action being taken against that person under our usual disciplinary processes. Breaches may result in dismissal for gross misconduct for employees and immediate contract termination for non-employees.