H&H Group PLC

Data Protection Information Governance Framework

Framework Dated / Reviewed:	**22 May 2018**
Adopted / Reviewed by […]:	**Roger Blake**
Date of Next Review:	**22 September 2018**
Directorate:	

Contents

Clause **Page**

1. **Data Protection Policy**

1.1. Importance of Data Protection

In order to operate as an organisation we hold Personal Data about employees, suppliers, volunteers, members and their family members, and other individuals. The use of personal data is governed by the General Data Protection Regulation (the "**GDPR**"). We take data protection very seriously and understand the impact that data breaches and misuse of data may have on data subjects as well as on our activities. Compliance with this policy is necessary for us to maintain the confidence and trust of those whose personal data we handle.

Non-compliance with this policy by employees could in certain circumstances constitute a serious disciplinary matter.

1.2. Who this Policy applies to

This policy applies to employees, consultants, temporary / agency staff, volunteers and anyone acting on behalf of H&H Group PLC. In this policy, reference to "employee" includes reference to any consultants, temporary / agency staff, volunteers and anyone acting on behalf of H&H Group PLC.

1.3. This Policy Statement

The aim of this policy statement is to give you a basic understanding of the data protection laws, our responsibility in respect of data protection practice, your rights and obligations and to explain why privacy is so important to us. It applies to all actions we take which involve the processing of and working with personal data. This policy has been approved by the board/executive/approving body within H&H Group PLC.

1.4. Data Protection Representative

Our Data Protection Representative is Roger Blake. Please feel free to contact him at any time if you have questions or concerns about the operation or interpretation of this policy. His contact details are as follows:

Roger Blake, H&H Group Services, 01228 406335
roger.blake@hhgroupplc.co.uk

1.5. What do I need to know about Data Protection?

1.5.1. Data protection legislation is not intended to prevent processing of personal data but to ensure it is done fairly and lawfully and in a way which does not adversely affect an individual.

1.5.2. We will process your personal data in accordance with the data protection laws. Processing includes obtaining, recording, holding, reading, using or destroying personal data.

1.5.3. The GDPR regulates the processing of personal data. Personal data is information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier, which include names, identification numbers, location data or other factors such as

the physical, genetic, biometric, mental, economic or social identity of a natural person. Data about businesses or organisations is not covered by the GDPR but data about their directors, partners, employees, customers and suppliers is.

1.5.4. We will process personal data in accordance with the GDPR and good data protection practice and will only use personal data for the purpose(s) it was intended for. We will keep a processing record of all processing of personal data we perform. We will make sure our fair processing notices are up to date and reflect the processing activities we undertake.

1.5.5. We will store personal data in a safe and secure manner and only people who really need to use it as part of their work responsibilities will have access to it. We will keep personal data only as long as is necessary for the purpose(s) it was collected for. Once personal data is no longer required, we will take reasonable steps to delete, destroy or erase it.

1.5.6. We will keep personal data up to date. Where a data subject reports an inaccuracy in the personal data we hold, we will correct it (unless we know the information is correct) and will inform any recipients of that personal data of the amendments.

1.5.7. We will avoid collecting special categories of personal data or criminal data unless absolutely necessary. If we do collect it, we will take extra measures to ensure it is kept safe and secure (see section 12.3 below).

1.6. Keeping data secure

1.6.1. We will process personal data securely by ensuring the confidentiality, integrity and availability of personal data is kept secure. We will ensure the level of security we use is appropriate to the risks arising out of the processing.

1.6.2. We have put in place a variety of policies and procedures which will keep data secure by providing guidance for our staff and contractors as to how personal data should be stored in order to reduce, as far as reasonably possible, the risks involved in processing personal data.

1.6.3. We will work together with our IT team to ensure that where our staff need to take electronic equipment containing personal data out of the office environment, the device contains security to keep the personal data safe and secure. Please refer to our IT & Communications Policy as well as Section 19 Home Working and Working Away from the Office, and Section 20 BYOD.

1.6.4. We have put in place other organisational and physical security measures to protect personal data. Staff and contractors must take particular care if they process personal data whilst working from home or away from the office. [*link to Home Working procedure*].

1.7. Requests for data

1.7.1. Individuals are entitled to make a request to us for a copy of the personal data that we hold about them. Requests should describe the information sought. Where we receive requests for personal data we will answer the request without undue delay and normally within one calendar month of receipt. *[link to Subject Access Request procedure].*

1.7.2. All data subject access requests will be considered properly. If applicants are unhappy with the way we handle requests, they should let us know using the complaint form found on our website.

1.7.3. Occasionally other bodies may ask for access to personal data we hold such as the police, the tax authorities and other enforcement agencies. Such requests should be referred to the Data Protection Representative [*link to Third Party Requests for Data procedure*.]

1.8. Other rights

1.8.1. Data subjects have a number of rights including a right to erasure, a right to data portability, a right to object to certain processing, a right to restrict processing in certain circumstances and a right to prevent automated decision making in certain circumstances, a data subject may request that the processing of their personal data be restricted. If you receive such requests, please refer it to the Data Protection Representative [*link to Data subject rights*].

1.8.2. We are committed to ensuring data subject rights are upheld and we will work hard to make sure these rights can be exercised.

1.9. Sharing Data with other people/organisations

We will not send personal data to a third party or another organisation unless the data subject has given us their authority to do so or we are otherwise permitted by law. We will take care to consider whether the data subject has given authority to their data being passed to another organisation before we transmit the data. Where data is being sent to an organisation for them to process the data either on their own behalf or for us, we will carry out due diligence on that organisation to make sure they have adequate data protection standards and processes. We will carry out due diligence, put in place contracts and/or data sharing protocols to govern the use of data by the third party to ensure compliance with all relevant legislation and guidance.

1.10. Staff, Customer, Supplier and Tenant Data

In the course of normal business operations we will collect and process various personal data about employees, suppliers, customers and tenants, including special category personal data. This information will be retained for the period set out in the data retention policy. We will process this data in accordance with the relevant fair processing notices.

1.11. Training

We will provide all staff and temporary workers with appropriate data protection training to make sure that data protection issues are dealt with properly and in

accordance with this policy and the law. We will make sure staff, temporary workers and workers at our processors have adequate training for their roles.

1.12. Data Retention and Destruction

Personal data will be retained by us as long as we need to process it or for as long as the law requires us to keep it. When we no longer need data we will delete or destroy it in accordance with good data protection practice. Where we use third party contractors to delete or destroy data, we will only use contractors who can demonstrate relevant experience and accreditations.

1.13. Data breaches

A data breach is a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed. In the event of a data breach, the Data Protection Representative shall log the breach, deal with it and resolve any issues arising out of the breach. *link to Data Security Breach Notification*.

1.14. Transferring Data Outside the EEA

We do not intend to transfer personal data outside the EEA. Where it is necessary to do so we will ensure any such transfer is carried out in accordance with the requirements of the GDPR to ensure that the level of protection to data subjects guaranteed by the GDPR is not undermined by any such transfer.

In the event that the United Kingdom leaves the European single market, we shall ensure that any transfer of personal data overseas is transferred in accordance with all applicable data protection legislation in place at the time of such transfer.

1.15. Changes to this Policy

We reserve the right to change this policy at any time where it is appropriate for us to do so; we will notify individuals of these changes.

In the event that the United Kingdom leaves the European single market, we will ensure that we comply with any new data protection legislation that is enacted as a result.

2. Data Protection Information Governance Framework Background

2.1. Introduction

2.1.1. This data protection information governance framework (the Framework) deals with the roles and responsibilities of H&H Group Plc, its subsidiaries and its staff with regard to the processing of personal data.

2.1.2. References to "you" and "your" in this Framework refer to employees of H&H Group Plc and references to "we", "us" or "our" refer to H&H Group Plc itself.

2.1.3. We process personal data about a range of data subjects, including employees, customers, clients and suppliers. We process personal data for a number of purposes such as maintaining records and

accounts, promoting goods and services as well as employee administration and the management of the business. It is critical to H&H Group Plc that we are able to use personal data in this way. In order to continue to be able to do so, we must comply with the GDPR.

2.1.4. Our Data Protection Representative is Roger Blake. If you have any questions regarding this Framework or questions regarding our data protection obligations, please contact Roger Blake or in his absence the Chief Executive Officer.

2.2. Policy on Personal Data

2.2.1. We endeavour to ensure that personal data is processed in accordance with the GDPR and in particular the six principles contained in the GDPR.

2.2.2. We have put in place systems of work and procedures to ensure that we comply with the GDPR. We aim to provide all employees with sufficient information, instruction and training as is necessary in order to identify personal data and process it appropriately.

2.2.3. Our directors have agreed this Framework. Its success depends on co-operation and the involvement of you and your colleagues to help meet its requirements.

2.2.4. This Framework will be reviewed at regular intervals and revised where it is considered appropriate to do so having regard to legislative change, codes of practice, guidance from or approved by the Information Commissioner's Office ("**ICO**"), good data protection practice and case law.

2.2.5. **Any breach of this Framework will be taken seriously and may result in disciplinary action.**

2.2.6. You have a duty to ensure that you are fully aware of this Framework and that you comply with its directions.

2.2.7. If you have any questions or queries in relation to this Framework, you should contact the Data Protection Representative.

2.2.8. We use a number of terms in this Framework such as "Data", "Data Subjects" and "Personal Data". These are defined in Appendix 1 of this Framework.

3. Legal obligations on Processing

3.1. In order to process personal data legally we must comply with the six Data Protection Principles. These state that personal data must be:

3.1.1. processed fairly, lawfully and in a transparent manner (*lawfulness, fairness and transparency*);

3.1.2. obtained for specified, explicit and lawful purposes and processed compatibly with those purposes (*purpose limitation*);

3.1.3. adequate, relevant and not excessive for the purposes for which it is processed (*data minimisation*);

3.1.4. accurate and up to date and every reasonable step must be taken to erase or rectify inaccurate data without delay (*accuracy*);

3.1.5. kept in a form which enables identification of individuals no longer than necessary for the purposes for which it is processed (*storage limitation*); and

3.1.6. processed subject to appropriate security measures (*integrity and confidentiality*).

4. **Data Processing Representative**

4.1. The contact details of the Data Protection Representative are

Roger Blake, H&H Group Services, 01228 406335
roger.blake@hhgroupplc.co.uk

We shall publish the contact details and inform the ICO of these contact details.

4.2. We will circulate the name and contact details of the Data Processing Representative to all members of staff who are involved in, or may become involved, data processing operations. The Data Protection Representative will report to the Chief Executive Officer of our organisation.

4.3. The Data Protection Representative will be the main contact for Data Subjects who have any issue relating to the processing of their personal data or who wish to exercise any of their rights as Data Subjects pursuant to the GDPR (see section 14 below).

4.4. The Data Protection Representative shall fulfil at least the following tasks:

4.4.1. to inform and advise us and any third party processor of our obligations pursuant to the GDPR and other relevant and applicable data protection laws;

4.4.2. to monitor:

4.4.2.1. compliance with the GDPR and other relevant and applicable data protection laws;

4.4.2.2. our policies and those of any third party processor relating to the processing of personal data, including assigning responsibilities, raising awareness and training staff or being responsible for the training of those involved in processing operations; and

4.4.2.3. related audits;

4.4.3. where required, to provide advice relating to data protection impact assessments (see section 7.14) and monitoring performance of those data protection impact assessments;

4.4.4. to co-operate with the ICO or any other supervisory authority; and

4.4.5. to act as the contact point for the ICO or other supervisory authority on issues relating to processing, including any prior consultation (see section 7.16 below), and to consult, where appropriate, on any other matter.

The Data Protection Representative must, in the performance of their tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

4.5. We must ensure (or any third party processor must ensure) that the Data Protection Representative is involved, in a proper and timely manner, in all issues relating to the protection of personal data.

4.6. We will (or any third party processor will) support the Data Protection Representative to perform their tasks by providing the necessary resources and allowing them to maintain their expert knowledge relating to data protection matters. This may include appointing additional staff to support and assist the Data Protection Representative, or ensuring that the Data Protection Representative can attend all relevant and necessary training.

4.7. The Data Protection Representative will be bound by an obligation of confidentiality concerning the performance of their tasks.

5. **Documentation**

5.1. In our to demonstrate our compliance with the accountability principle under GDPR we are required, or it is best practice, to maintain various documentation, including the documents listed below and any other documents referred to in this Framework:

5.1.1. A processing record (see section 5.2 below);

5.1.2. A data breach log (see Annex 6 below);

5.1.3. A data protection policy (this Framework);

5.1.4. Fair processing notices; and

5.1.5. Data protection impact assessments for certain projects (see sections 7.14 to 7.25 below)

5.2. Processing Record

5.2.1. We must maintain a written record of our processing activities, if we process personal data. A template processing record is set out in Appendix 2 to this Framework and is maintained by the Data Protection Representative. The processing record must contain as a minimum the following information for each processing activity involving personal data:

5.2.1.1. the name and contact details of the data controller (and, where applicable, the joint controller, the data controller's representative and the data protection representative);

5.2.1.2. the purposes of the processing;

5.2.1.3. a description of the categories of data subjects and the categories of personal data;

5.2.1.4. the categories of recipients to whom the personal data have been or will be disclosed (including, where applicable, recipients in third countries or international organisations);

5.2.1.5. transfers of personal data to a third country or international organisation (where applicable), including the identity of the third controller or international organisation and, where applicable, the documentation of suitable safeguards;

5.2.1.6. the proposed time limits for erasure of the different categories of personal data, where possible; and

5.2.1.7. a general description of the technical and organisational security measures taken to protect the personal data.

5.2.2. The processing record shall be maintained by the Data Protection Representative who shall ensure that it is accurate and up to date. The processing record is available at H&H Group, Borderway Mart, Carlisle, CA1 2RS. If you are aware that the processing record is incorrect or out of date please inform the Data Protection Representative immediately.

5.2.3. The processing record must be made available to the ICO or relevant supervisory authority if requested.

5.3. Data Breach Log

5.3.1. Please see Annex 6 for further details on the information that should be recorded in the data breach log.

5.3.2. The data breach log shall be maintained by the Data Protection Representative who shall ensure that it is accurate and up to date. The data breach log is available at H&H Group, Borderway Mart, Carlisle, CA1 2RS. If you are aware that the data breach log is incorrect or out of date please inform the Data Protection Representative immediately.

5.3.3. The data breach log shall be made available to the ICO or relevant supervisory authority if requested.

5.4. Data Protection Information Governance Framework

5.4.1. This Framework shall be maintained by the Data Protection Representative who shall ensure that it is accurate and up to date. If you are aware that this Framework is incorrect or out of date please inform the Data Protection Representative immediately.

5.5. Fair processing notices

5.5.1. Please see section 11 below for further information on the contents of the fair processing notice and how the information within it should be made available to Data Subjects.

5.6. Data protection impact assessments

5.6.1. Please see sections 7.14 to 7.25 below for further information on when Data Protection Impact Assessments must be carried out and what they must contain.

6. Data Protection Best Practice

6.1. We must process personal data in accordance with the GDPR. We are responsible for:

6.1.1. explaining to all relevant staff the importance of data protection;

6.1.2. providing staff (including temporary staff) with adequate training (where necessary), information, instruction and supervision to ensure personal data is processed in accordance with the GDPR;

6.1.3. assuming overall responsibility for compliance with the GDPR;

6.1.4. selecting someone to be responsible for ensuring compliance with the GDPR and making this person known to staff. This person is Roger Blake, who is the Data Protection Representative; and

6.1.5. maintaining a record of how personal data is kept and processed; and

6.1.6. maintaining other documentation including a data breach log (please see section 5).

6.2. You should:

6.2.1. be aware of the issues regarding data protection and contact the Data Protection Representative if you have any queries in relation to this Framework;

6.2.2. consider the rights of data subjects who may be affected by your data processing actions;

6.2.3. always process personal data in accordance with this Framework;

6.2.4. report any data subject access requests, applications in respect of other data subject rights or other questions regarding data protection to the Data Protection Representative;

6.2.5. report any actual or suspected breach of this Framework to the Data Protection Representative immediately; and

6.2.6. report any Personal Data Breach to the Data Protection Representative immediately you become aware of it.

7. Processing Personal Data

7.1. All personal data should be processed in accordance with the GDPR and this Framework.

7.2. Personal data is data relating to an individual. It includes employee data, temporary worker / work placement / student / intern data, supplier data, customer

and client data. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations will be covered.

7.3. Examples of personal data are employee details including employment records, (see section 16 - Employee Personal Data), any third party data, for example information relating to an employee of a supplier or any information gathered about a customer. Recorded telephone conversations, notes or opinions relating to an individual or the suitability of a particular individual for a task, as well as photographs taken of staff, suppliers or customers or CCTV images can all be personal data.

7.4. You will process personal data when you obtain, record or hold the information or data or carry out any operation with the personal data. The following arrangements could involve data processing (this is a non-exhaustive list):

7.4.1. provision of payroll services;

7.4.2. database management;

7.4.3. use of your own mobile phone/social media account to discuss work issues;

7.4.4. use of your own tablet, laptop, smart phone, mobile phone or digital camera to carry out work;

7.4.5. taking and storing photographs of job applicants, employees, customers, including taking photographs of you or your colleagues in the office;

7.4.6. the disposal of old computer equipment containing personal data;

7.4.7. the disposal of old office equipment such as filing cabinets which contain paper records detailing personal data;

7.4.8. scanning of personnel, pension or customer records;

7.4.9. office relocation activities involving the movement of personal data records; and

7.4.10. disposal of confidential waste containing personal data.

7.5. You should assume that whatever you do with personal data will be considered to involve processing it and must be carried out in accordance with the requirements of the GDPR. You should therefore only process data if one of the processing conditions set out in the GDPR applies. The conditions most likely to apply to processing activities are:

7.5.1. you have consent to do so. If you are relying on consent to process the personal data you must make sure that the specific consent given covers you for the precise reason you want to process the personal data. Any consent relied on must be clear, specific as to the use intended and unambiguous.

7.5.2. it is necessary to fulfil a contractual obligation or as part of the employer/employee relationship (for example, processing the payroll). It would also be necessary to process a customer's personal data if they placed an order with us. We would need to keep address details to fulfil our obligation to supply the goods or services and we would need to keep some record of the payment made. These uses would also be necessary to fulfil a contractual obligation; or

7.5.3. there is another legitimate reason to process the personal data (for example, in the course of an investigation into an individual's performance for a particular organisation). If you rely on this condition for processing personal data, we will need to consider what that legitimate interest is, record it in the Processing Record and notify a Data Subject of the legitimate interests if we receive a data subject access request in respect of the personal data. When we rely on the legitimate interests condition we must carry out a three stage test called a Legitimate Interest Assessment (LIA). First, the processing must be necessary, second, we must identify the legitimate reason for processing (this can be the controller's or a third party's. Finally we must carry out a balancing test between the legitimate rights of the controller or relevant third party and the interests and rights and freedoms of the data subject. Only if the individual's interests and rights and freedoms are overridden by the controller's (or relevant third party's) legitimate interests can we rely on this basis for processing the personal data. We will keep a record of all LIAs we perform.

7.6. If you are not sure if one of the conditions in paragraph 7.5 is satisfied, you should contact the Data Protection Representative before processing the personal data to ensure that H&H Group Plc can legally carry out the proposed activity. If the personal data to be processed includes special category personal data, you must make sure you can satisfy a valid special category data processing condition to process it. See paragraph 12.3 for further information.

7.7. We will take every reasonable step to ensure that data is kept accurate and up to date.

7.8. We will regularly review files and the data we process to make sure we keep the data we process to a minimum.

7.9. Processing personal data relating to a criminal conviction or offence

7.9.1. We must only process personal data relating to criminal convictions and offences or related security measures when that processing is carried out under the control of official authority or is authorised by law.

Data Security

7.10. When processing personal data, we must ensure that we implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risks involved in processing such data. This may include, for example, pseudonymising certain personal data (i.e. taking identifying fields in a database and replacing them with artificial identifiers), so that the data is anonymous to the people who receive and hold it, or encrypting certain personal data. Implementing appropriate technical and organisational measures also means that we must:

7.10.1. be able to restore the availability and access to personal data in a timely manner, in the event that there is a physical or technical incident involving any personal data (*disaster recovery*);

7.10.2. have a process in place for regularly testing, assessing and evaluating the effectiveness of these measures to ensure the security of our data processing; and

7.10.3. ensure that, by default, only the personal data which is necessary for each specific purpose of processing is in fact processed.

We are always looking for ways to improve the security of our processing operations. If an employee has any concerns or suggestions in relation to the security of our processing operations, or the technical and organisational measures adopted by H&H Group Plc, they should contact the Data Protection Representative. Please see section 12 for a more complete description of the data security processes.

Privacy by Design and Data protection impact assessment

Privacy by Design

7.11. Privacy by Design means that we are required to build privacy into the design, operation and management of any system, hardware, software, business practice, protocol or operation that processes personal data. The principle of Privacy by Design requires that our default position is to apply the strictest privacy settings to any new product or service that we are proposing to use which processes personal data automatically. Privacy settings should always be set to the most private setting possible. If a Data Subject is able to control privacy settings, we must not require them to adjust the privacy settings to increase them.

7.12. Privacy assurance and Privacy by Design must be embedded into our day-to-day operations, and should not be a mere afterthought. It forms a fundamental element of our organisation's risk structure. It should involve input from members of our regulatory, organisational and technical teams.

7.13. By ensuring that privacy is at the forefront of our thoughts and is embedded throughout the entire organisation, we will not only reduce the risk of a Personal Data Breach, but we will reduce the time, effort and cost spent dealing with privacy concerns that arise.

Data protection impact assessments

7.14. If we consider that a particular type of processing is likely to result in a high risk to the personal data of Data Subjects, we must carry out an assessment on the impact that the proposed processing will have on the protection of personal data. We may conduct a single assessment on a number of different processing operations that each present similar high risks.

Examples of where we would be required to conduct an impact assessment include:

7.14.1. if we process, on a large scale, sensitive personal data, including personal data relating to criminal convictions or offences; or

7.14.2. if we systematically monitor a publicly accessible area on a large scale (this may be the case, for example, if we have many CCTV cameras which monitor public areas near our premises).

7.15. As a minimum, a data protection impact assessment must contain:

7.15.1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest(s) we are pursuing;

7.15.2. an assessment of the necessity and proportionality of the processing operations in relations to the purpose. In other words, do we need to process data in this particular way, and can it be done in a less intrusive, or more restricted manner?;

7.15.3. an assessment of the risks to the rights and freedoms of data subjects; and

7.15.4. the measures envisaged to address such risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

7.16. We will conduct impact assessments on the processing operations that the ICO publicly list as requiring impact assessments.

7.17. We may, when conducting an impact assessment, seek the views of Data Subjects on the intended processing operation.

7.18. If there is a change of the risk presented by a particular processing operation, we will carry out a further review to assess whether the processing is being performed in accordance with the impact assessment.

7.19. If a processor is involved in the processing activity we should ask for their assistance in completing the DPIA. They are under a legal obligation to help us in this regard.

7.20. Data protection impact assessments should be carried out using the form set out in Appendix 7.

Prior consultation

7.21. If an impact assessment indicates that any processing operation would, in the absence of measures taken by us to mitigate the risk, result in a high risk to the rights and freedoms of Data Subjects, then we must consult with the ICO or relevant supervisory authority.

7.22. If the ICO or relevant supervisory authority deems that the proposed processing would infringe the GDPR, for example if we have insufficiently identified or mitigated the risks, the ICO or relevant supervisory authority will provide us with written advice. This should be provided within eight (8) weeks of the ICO receiving our request for consultation, but the ICO or relevant supervisory authority may extend this period by six (6) weeks, taking into account the complexity of the proposed processing.

7.23. If we consult the ICO or relevant supervisory authority in relation to any proposed processing, we must provide it with:

7.23.1. (where applicable) the respective responsibilities of the data controller, joint controllers (if any), and the data processors involved in the processing;

7.23.2. the purposes and means of the intended processing;

7.23.3. the measures and safeguards provided to protect the rights and freedoms of Data Subjects pursuant to the GDPR;

7.23.4. the contact details of the Data Protection Representative (if applicable);

7.23.5. the data protection impact assessment; and

7.23.6. any other information that the ICO or relevant supervisory authority may require.

7.24. We may be required by law to consult with, and obtain prior authorisation from, the ICO or relevant supervisory authority in relation to processing for tasks carried out in the public interest, including in relation to social protection and public health.

7.25. The Data Protection Representative shall be responsible for determining whether any consultation with the ICO or relevant supervisory authority is required and shall be responsible for liaising with the ICO or relevant supervisory authority in respect of any such consultation.

Using Data Processors

7.26. Where we use a third party to process any personal data on our behalf (for example, if we use a contractor to destroy confidential information which contains personal data or if we outsource pensions administration), we must ensure that they provide sufficient guarantees that they do, and will continue to, implement appropriate technical and organisational measures to ensure compliance with the GDPR and protect the personal data of Data Subjects.

7.27. We must not engage any third party to undertake any processing on our behalf unless and until we have entered into a valid, binding written contract with that third party. Any such contract must include, as a minimum:

7.27.1. the subject matter and duration of the processing that the third party will undertake;

7.27.2. the nature and purpose of the processing;

7.27.3. the type of personal data and categories of data subjects;

7.27.4. our rights and obligations under the contract;

7.27.5. that the processor will only process personal data on our written instructions;

7.27.6. that persons authorised to process the personal data on behalf of the third party are subject to an appropriate obligation of confidentiality;

7.27.7. that the processor will take all measures required by the GDPR relating to the security of processing;

7.27.8. that the processor will only engage another processor in certain circumstances (see paragraph 7.28 below);

7.27.9. that the processor will assist us (so far as it is possible) in responding to a request made by a Data Subject in exercising any of its rights under the GDPR (see paragraph 14.3 below);

7.27.10. that the processor will assist us in complying with certain of our obligations set out in the GDPR, including by:

7.27.10.1. ensuring the security of the processing;

7.27.10.2. notifying us, without undue delay, after becoming aware of any Personal Data Breach and co-operating with us to notify the ICO or relevant supervisory authority and any affected Data Subject of the Personal Data Breach;

7.27.10.3. assisting us to remedy and rectify any such Personal Data Breach;

7.27.10.4. assisting us if and when we carry out any data protection impact assessment (see paragraph 7.15 above); and

7.27.10.5. assisting us and co-operating with us if we are required to consult with the ICO or relevant supervisory authority in relation to any high risk processing;

7.27.11. that the processor will, at our discretion, delete or return all of the personal data to us when it ceases to process personal data on our behalf;

7.27.12. that the processor will delete any existing copies of the personal data when it ceases to process personal data on our behalf (unless it is required by law to retain a copy); and

7.27.13. that the processor will make all information available to us which is necessary to demonstrate its compliance with its contractual obligations, and that it will allow for and contribute to audits and inspections conducted by us or on our behalf.

7.28. A third party processing personal data on our behalf must not use another data processor without first obtaining our prior written authorisation. The Data Protection Representative must provide any such authorisation].

7.29. If a third party is authorised by us to use another processor to carry out specific processing activities on our behalf, that additional processor must be subject to the same data protection obligations as the third party is subject to with us. We should ask the third party to provide a copy of the contract it proposes to enter into with the additional processor before we provide any authorisation.

8. **Consent**

8.1. Where we rely on consent to process personal data we must abide by the terms of this section 8.

8.2. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of a Data Subject's agreement to the processing of their personal data.

8.2.1. Examples of consent include a written statement by a Data Subject (including by electronic means). This could include ticking a box when visiting a website or another statement or conduct which clearly indicates, in the particular context, the Data Subject's acceptance of their personal data being processed in a particular way.

8.2.2. Silence, pre-ticked boxes or inactivity by a Data Subject must not, at any point, be construed as a Data Subject providing their consent to the processing of their personal data. If you have any doubts as to whether a Data Subject has validly consented to the processing of their personal data, please contact the Data Protection Representative immediately. You must not process a Data Subject's personal data until we are satisfied that consent has been validly obtained.

8.3. Consent must cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent must be given for all of those purposes. As an example, if a Data Subject has provided their consent to us processing their personal data for administrative purposes, we cannot process their personal data for marketing purposes unless we have specific consent from the Data Subject to do so.

8.4. The consent of children needs to be dealt with carefully, as they may be less aware of the risks, consequences and safeguards concerned, as well as their rights, in relation to the processing of their personal data. Under the (Data Protection Bill] which covers derogations under the GDPR into force in the UK, a child is defined as someone who is 13 or under. You should, always ensure that the consent of the holder of parental responsibility for a child is obtained, particularly with regard to the use of personal data for the purposes of marketing, creating personality or user profiles and when offering services directly to a child. The consent of the holder of parental responsibility for a child should not be necessary in the context of preventive or counselling services offered directly to a child.

If you have any concerns or queries regarding the consent of child with regard to the processing of their personal data, you must contact the Data Protection Representative immediately.

8.5. If processing is based on a Data Subject's consent, we must be able to demonstrate that the Data Subject has given their consent to the particular processing operation (see section 8.3 above). A Data Subject should be aware of the extent to which their consent is given. We must keep a record of the consent wording used for each individual

8.6. If we use a pre-formulated declaration of consent for a Data Subject to use, this declaration must be:

8.6.1. in an intelligible and easily accessible form;

8.6.2. in clear and plain language;

8.6.3. without any unfair terms; and

8.6.4. if given in the context of a written declaration which also concerns other matters, presented in a manner which is clearly distinguishable from those other matters.

Any part of such a declaration which infringes any of 8.6.1 to 8.6.4 above shall not be binding on the Data Subject.

8.7. For consent to be informed, a Data Subject should be aware, at the very least, of the following:

8.7.1. Our identity as data controller; and

8.7.2. The purpose(s) of the processing for which the personal data are intended.

The Data Protection Representative shall be responsible for the provision of any pre-formulated declaration of consent that we use. In no circumstances, without the prior written consent of the Data Protection Representative, shall any variation or amendment to the pre-formulated declaration of consent be permitted.

8.8. Consent will not be regarded as freely given if the Data Subject cannot refuse or withdraw their consent without suffering any detriment.

8.9. Prior to giving consent, a Data Subject must be informed that they have the right to withdraw their consent at any time. It must be as easy for a Data Subject to withdraw their consent as it is to give their consent.

8.10. The withdrawal of a Data Subject's consent does not affect the lawfulness of any processing based on consent prior to the withdrawal. The Data Subject must be informed of this fact prior to giving their consent.

8.11. Consent must not be regarded as freely given if the Data Subject has no genuine or free choice.

8.12. Consent is presumed not to be freely given if it does not allow separate consent to be given to different data processing operations despite it being appropriate in an individual case.

8.13. Consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on consent despite such consent not being necessary for such performance.

8.14. If there is a clear or significant imbalance between the Data Subject and us as controller (for example, the employer / employee relationship), consent may not provide a valid legal ground for the processing of that Data Subject's personal data.

9. **Information on personal data, Instruction and Supervision**

9.1. A copy of this Framework will be kept at H&H Group, Borderway Mart, Carlisle, CA1 2RS.

9.2. Data protection advice is available from the Data Protection Representative who will arrange for advice from external advisers if necessary.

9.3. We will ensure that all new staff, particularly those with access to personal data, are trained on our Framework as soon as possible after they are recruited. The level of training for each individual employee will depend on the level of access and responsibility for processing personal data. Please also see below (*Competency for Tasks and Training*).

9.4. Temporary staff, work placement students, interns and new staff who will have access to personal data will receive data protection training before they are allowed to process personal data. Temporary staff, work placement students, interns and new staff must not be allowed to carry out activities involving the processing of personal data until such training has been completed.

9.5. If you feel that you need additional training for a particular task or a refresher you should contact the Data Protection Representative who will discuss this with you and arrange for additional training if necessary.

9.6. If you consider that any task or work you have been asked to undertake involves the processing of personal data and you are unsure whether or not the task or work would be in breach of the GDPR or other laws, you should check this with the Data Protection Representative.

Competency for Tasks and Training

9.7. We recognise that our employees are a key factor in supporting our effective and efficient operation and helping us to comply with data protection laws and good practice. We are committed to ensuring that staff receive relevant training and development to help fulfil our legal and good practice obligations regarding the processing of personal data.

9.8. In the first instance, staff will receive an appropriate "on the job" induction into the organisation. The induction will cover data protection. The level of training will be dependent on that member of staff's position.

9.9. All new employees will undertake a probationary period under the supervision of an experienced employee until they achieve the appropriate standards and efficiency required for our employees. Additional training on data protection issues may be provided as appropriate.

9.10. Staff should only process personal data when they have received adequate training to do so. This applies equally to full time, part time and temporary employees, including work placement students and interns. If a staff member considers that he or she needs further or refresher data protection training to carry out a task allocated to them, they should notify the Data Protection Representative who will consider the request.

9.11. It is important we keep a record of data protection training undertaken by employees. This record is kept by Human Resources. Employees must notify us of

any data protection training they undergo so that we can keep their training records up to date. If an employee has received data protection training before they join the organisation, it is useful for us to know this, as it is important for us to understand the skill sets of our employees.

10. Monitoring the Use of Personal Data

10.1. We are committed to ensuring this Framework is put into practice and that appropriate working practices are being followed. To this end, the following steps will be taken:

10.1.1. all employees who deal with personal data will be made aware of data protection issues and encouraged to work towards continuous improvement in the way we process personal data;

10.1.2. employees who handle personal data on a regular basis or who process special category or criminal data or other confidential personal data will be monitored;

10.1.3. spot checks may be carried out by managers to ensure compliance with data protection laws and this Framework; and

10.1.4. the Data Protection Representative shall submit to the Chief Executive on a quarterly basis a report on, amongst other things, the level of compliance with or variance from good data protection practices. The directors/executives will consider what steps, if any, are necessary in order to improve data protection performance.

Complaints

10.2. Complaints on the way we have processed personal data may be received from:

10.2.1. employees;

10.2.2. suppliers;

10.2.3. customers; or

10.2.4. others whose personal data we handle.

Complainants should be encouraged to complete our Complaint Form set out in Appendix 5 below. However, complaints should be dealt with even if no complaint form is completed.

The Data Protection Representative will be responsible for investigating any complaints about our data protection practices in order to deal with any data protection breaches and to see what improvements can be made to prevent recurrences of such breaches. The results of such investigations will be reported to the Chief Executive who will be responsible for arranging for any improvements to be carried out.

11. Provision of Fair Processing Notices

11.1. We must provide fair processing information to Data Subjects relating to the processing of their personal data. The information we are required to provide

depends upon whether a Data Subject's information is collected from the Data Subject directly or if the information has been obtained from a source other than the Data Subject.

If we have obtained the personal data from the data subject

11.2. We must provide the Data Subject with the following information, to ensure fair and transparent processing:

11.2.1. who we are and our contact details;

11.2.2. the contact details of our Data Protection Representative;

11.2.3. the purposes of the processing and the legal basis for the processing;

11.2.4. if the processing is necessary for our (or a third party's) legitimate interests, what those legitimate interests are;

11.2.5. the recipients, or categories of recipients, of the personal data (if any);

11.2.6. whether we intend to transfer personal data outside the EEA, and what safeguards are in place;

11.2.7. the period that the personal data will be stored, or, if we cannot specify such a timeframe, the criteria we will use for determining such a period;

11.2.8. the Data Subject's right to:

11.2.8.1. access their personal data;

11.2.8.2. request the rectification or erasure of their personal data;

11.2.8.3. request that the processing of their personal data be restricted; and

11.2.8.4. their right to data portability (see paragraph 14.3.6 below);

11.2.9. that if the processing is based on their consent, that they have the right to withdraw their consent to the processing at any time (which will not affect the lawfulness of any processing based on their consent before it is withdrawn);

11.2.10. that they have the right to lodge a complaint with the ICO or relevant supervisory authority;

11.2.11. whether the provision of their personal data is a statutory or contractual requirement, or it is required to enter into a contract, as well as whether a Data Subject is *obliged* to provide their personal data and the possible consequences if they fail to provide such personal data; and

11.2.12. whether there will be any automated decision-making (including profiling) and the logic involved, as well as the significance and envisaged consequences of such processing for a Data Subject.

11.3. The Data Protection Representative shall be responsible for ensuring such information is provided to a Data Subject. If we intend to further process a Data Subject's personal data for a purpose which is different to that which the personal data was originally collected for, we must provide the Data Subject with information on this new purpose and with any other relevant information in paragraphs 11.2.1to 11.2.12 that may have changed.

If we have obtained a Data Subject's personal data from a source other than the Data Subject

11.4. We must provide the Data Subject with the same information as set out in paragraphs 11.2.1 to 11.2.12, with the exception of the information in paragraph 11.2.11 However, we must also inform Data Subjects of:

11.4.1. the categories of personal data concerned; and

11.4.2. the source from which their personal data originated, and, if applicable, whether it came from publicly accessible sources;

11.5. We must provide the information set out in paragraph 11.4 to a Data Subject within a reasonable period of obtaining the personal data, and in any event within one month.

11.6. If we are using the personal data for communicating with a Data Subject, then we must provide the information set out in paragraph 11.4 no later than the first communication with the Data Subject. This information can be provided in a number of ways including in a statement in our email footer, in an email with the Data Subject (if we are communicating with the Data Subject via email).

11.7. If we envisage disclosing personal data to another recipient, we must provide the information set out in paragraphs 11.4 to the Data Subject no later than when the personal data is first disclosed.

11.8. If we intend to further process a Data Subject's personal data for a purpose which is different to that which the personal data was originally collected for, we must provide the Data Subject with information on this new purpose and with any other relevant information in paragraph 11.4 that may have changed.

11.9. There are certain circumstances when we may not be required to provide the information in paragraph 11.4 to a Data Subject, including where the Data Subject already has the information. If you are uncertain as to whether or not the information should be provided to a Data Subject, or when it should be provided to a Data Subject, you should contact the Data Protection Representative.

12. **Data Security**

12.1. We shall:

12.1.1. take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data. The GDPR requires procedures and technologies to be implemented to maintain the security of all personal data from the point of collection to the point of destruction. The measures taken should be appropriate for the harm which will be caused by any such accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to

personal data. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

12.1.1.1. "**Confidentiality**" means that only people who are authorised to use the data can access it;

12.1.1.2. "**Integrity**" means that personal data should be accurate and suitable for the purpose for which it is processed; and

12.1.1.3. "**Availability**" means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore only be saved on our central computer system instead of individual PCs, laptops, smart phones and other employee owned devices;

12.1.2. ensure that staff who handle personal data are adequately trained and monitored;

12.1.3. ensure that passwords and physical security measures are in place to guard against unauthorised disclosures; and

12.1.4. where employees are allowed to work from home or use their own device for work, employees must ensure they comply with the IT and Communications Policy. Please also see section 19 – Home Working and section 20 - BYOD.

12.2. Paper Records

12.2.1. Manual data refers to paper and other non-digital personal data, records (such as copies of photographs or plans) which are recorded as part of a relevant filing system or with the intention that it should form part of such a system.

12.2.2. A filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. For example, this could include employment records stored alphabetically in a cabinet, or it could be a diary or desk workbook containing personal data. It is good practice to treat all personal data, however stored or held, in accordance with the principles set out in the GDPR.

12.2.3. We shall ensure that all written records containing personal data shall be reviewed in accordance with paragraph 12.2.4 and a record shall be kept of all such reviews.

12.2.4. Manual records containing personal data must be regularly reviewed in order to ensure that the data contained within them is accurate, not excessive, up to date and adequate for their purpose(s). In any event you should review manual records as and when they are periodically reviewed or retrieved for whatever purpose.

12.2.5. Any documents containing personal data or sensitive personal data should not be left on a desk on view when the desk is unattended.

12.2.6. If employees need to work away from the office they must either use their work laptop or their own device, provided they do so as set out in the Home Working and Working Away from the Office policy in section 19 and the BYOD policy set out in section 20.

12.3. Special Categories of Personal Data

12.3.1. We will:

12.3.1.1. take particular care of special categories of personal data and if we have access to such information, we will make sure we process it properly and in accordance with the GDPR;

12.3.1.2. unless the Data Subject is an employee, we will make sure we obtain the explicit consent of the individual before processing sensitive data relating to them. If explicit consent has not or cannot be obtained (for example, you cannot use consent as a reason to process employee data), we must ensure that before any special categories of personal data are processed, one of the other special categories of personal data processing conditions set out in the GDPR apply. If you are unsure, please contact the Data Protection Representative; and

12.3.1.3. store all special categories of personal data with adequate security measures to prevent unauthorised disclosure. Such measures will include lockable cabinets and password protection of automated data, pseudonymisation and encryption of such data.

12.3.1.4. ensure that our processes, procedures, systems and policies for processing special categories of personal data are regularly tested to ensure they are resilient, compliant with and appropriate for the GDPR. This will include ensuring that adequate disaster recovery plans are in place at all times and that our systems are regularly tested, assessed and evaluated for their effectiveness in keeping special categories of personal data secure.

12.4. Technical Security measures

12.4.1. We will ensure that all computers have protection against malicious software/viruses and that software is not installed and information is not downloaded without first being checked by our IT provider for viruses and other malware. We will keep up to date with patches, fixes and new releases to ensure that our systems are protected against known security issues. [Please refer to the IT & Communications Policy.

12.4.2. Personal data should always be stored electronically on our central computer system, rather than on local drives, devices or at home.

12.4.3. All computers and documents containing personal data should be password protected and all passwords should be kept secret at all times. Employee passwords should include a mixture of letters and numbers and must not be easy to guess or use common combinations - such as "1234". Employees must not use consecutive versions of the same password such as "Password 1", "Password 2". We will notify employees when we require them to change their password.

12.4.4. Employees should store devices containing personal data carefully if taken out of the work place. Laptops, tablets, smart phones and other mobile devices should be stored securely and not left unattended in cars, railway carriages, in public places or on top of desks or table tops at home left unattended overnight. [Please see section 19 for further information].

12.4.5. Employees should ensure that individual monitors are positioned so they do not show confidential information to passers-by or people sitting in adjacent seats in public places. This is particularly important if a PC displays employee, customer, supplier or sensitive data. PCs should be logged off when left unattended.

12.4.6. Where employees use a memory stick to store information they must use an encrypted memory stick provided by [the IT department]. Employees must not use unencrypted memory sticks to store personal data.

12.5. Organisational Security Measures

12.5.1. Manual records

Employees must keep manual records secure by the use of locked cabinets. Access to such records should be restricted to those employees whose job requires access. Where a manual record is in constant use, employees should take appropriate security measures. These could include securing such records during lunch breaks and outside office hours and positioning desks and screens to prevent inadvertent disclosure.

12.5.2. Telephone enquiries

If employees deal with telephone enquiries they should be careful about disclosing any personal data held by us. In particular they should:

12.5.2.1. check the caller's identity to make sure that information is only given to a person who is entitled to it;

12.5.2.2. suggest that the caller puts their request in writing if they are not sure about the caller's identity or where their identity cannot be checked; and

12.5.2.3. refer to the Data Protection Representative for assistance in difficult situations.

Particular care needs to be taken when speaking to parents / guardians if an enquiry is made about their child's personal data, as the parent / guardian may have no legal right of access to the information. [See section 14 on Data Subject Access Requests].

12.5.3. Building access

Building access codes, if applicable, should be kept secret and you should ensure that when you enter the code, it cannot be seen by any third party. Where security passes are in place all staff must wear their security passes at all times in a prominent, visible position. Do not hold the entry door open for individuals you do not know or who are not displaying a valid security pass. Any stranger seen in entry-controlled areas should be reported immediately to their line manager.

12.5.4. Storage

You must store personal data in a manner which enables it to be processed in accordance with the GDPR. Files should indicate what information they contain and should be readily accessible (provided appropriate security measures are taken) to enable data subject access requests to be handled in accordance with this Framework, see section 14 (Dealing with Data Subject Access Requests).

12.5.5. Deletion or destruction of data

12.5.5.1. Where personal data needs to be deleted or destroyed, adequate measures should be taken to ensure that such data is properly and securely disposed of. This will include the destruction of files and back up files and the physical destruction of manual files.

12.5.5.2. The sale or destruction of all IT equipment including PCs, laptops, smart phones and other mobile devices should be treated as a data processing activity. This will include even where a device or PC, laptop or device is found to be corrupted. Measures should be taken including the use of specialist contractors who have relevant accreditations to ensure data on IT equipment is forensically wiped.

12.5.5.3. Particular care should be taken with the destruction of manual sensitive data (written records) and this may include shredding or giving it to specialist contractors.

12.5.5.4. Where data is to be destroyed using third party contractors, due diligence should be undertaken in respect of such contractors including checking relevant accreditations to ensure that they cover the relevant activities and the checking of references. The destruction of data and equipment containing data is a data processing activity and we must ensure that a contract is in place which complies with our legal requirements in this regard (see sections 7.26 - 7.29.

12.5.5.5. All equipment or information destroyed shall be recorded using certificates of destruction which record the nature of the data, the reason for destruction, the date and method of destruction and the responsible contractor (if any) which shall be kept by the Data Protection Representative. Prior to destruction/deletion the responsible person must satisfy himself/herself that the data is no longer required, that no work is outstanding on or using the data and that no litigation or internal or external investigation is pending where such data would be required as evidence.

12.6. Security Policy Updates

We shall ensure all security policies and procedures are regularly monitored and reviewed to ensure that data is being kept securely. Policies and procedures shall be reviewed against good data protection practice including ICO and other regulatory guidance and case law. Where policies and procedures are found to be inadequate, prompt and appropriate action shall be taken in order to rectify such inadequacies. This shall include a review of the security sections and the consideration and implementation of replacement provisions to rectify such inadequacies. We shall notify users of any changes in the Framework.

13. Personal Data Breach, Notification and Reporting

13.1. Introduction

We shall ensure that personal data is stored and used in accordance with this Framework and the law. However, breaches may occur despite our best efforts. We are under a statutory obligation to report Personal Data Breaches to the ICO or relevant supervisory authority. It is therefore essential that on discovering a breach has occurred, the breach is reported in accordance with this Framework to ensure that the impact of the breach on data subjects is minimised and our liability for the breach can be limited as much as possible. Reporting and thorough investigation of incidents also helps to ensure that potential risks and problems are identified early and appropriate changes are made to minimise the possibility of future Personal Data Breaches occurring.

13.2. What is a Personal Data Breach?

13.2.1. The sixth data protection principle provides that appropriate technical or organisational measures are used to ensure the appropriate security of personal data, including against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

13.2.2. A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored or otherwise processed.

13.2.3. A key feature of a Personal Data Breach is the release (no matter how caused) of personal data to a third party who is not authorised to access, view, hold or otherwise process the information. Examples of Personal Data Breaches would be:

13.2.3.1. an employee leaving a piece of personal data about another employee (such as their address, date of birth etc.) on a desk when the employee leaves the desk so that other employees who do not have permission to view the information can see it;

13.2.3.2. the sending of an e-mail containing personal data (for example a database) to a third party that is not entitled to see it, for example, by entering the wrong email address;

13.2.3.3. the loss of a folder of papers or an electronic device such as a memory stick containing personal data in a public place; and

13.2.3.4. the theft of a laptop, tablet, smart phone, mobile or digital device (such as a camera) containing personal data, such as a database or e-mails.

13.3. What should I do if I think a Personal Data Breach has occurred?

13.3.1. If there is a Personal Data Breach, we must notify the ICO or relevant supervisory authority, without undue delay, and where feasible, no later than 72 hours after having become aware of it.

13.3.2. We are required to notify the ICO or relevant supervisory authority unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. the disclosure only of a Data Subject's name or email address). The Data Protection Representative shall be responsible for determining whether the Personal Data Breach is likely to result in a risk to the rights and freedoms of natural persons.

13.3.3. If you know or suspect that a Personal Data Breach may have occurred, regardless of who is at fault, this must be reported to the Data Protection Representative **immediately**. In the Data Protection Representative's absence, the Personal Data Breach should be reported to the Chief Executive.

13.3.4. Regardless of the size of the Personal Data Breach, this should still be reported on a Security Breach Incident Form in accordance with paragraph 13.4 below.

13.3.5. You should also notify the Data Protection Representative if there is a 'near-miss'. In other words, where there is a data security incident but it does not result in injury, dissatisfaction, loss or damage of a tangible asset, loss or damage to the reputation, mission or interests of someone or financial injury or harm. Reporting of near misses can help prevent actual incidents of injury, loss or damage occurring. A near miss would occur when, for example, a memory stick is lost which contains personal data but is known to be encrypted.

13.3.6. The Data Protection Representative shall ensure that all Personal Data Breaches are promptly and adequately investigated, notified to the ICO as soon as possible (where appropriate), resolved and documented.

13.3.7. The Data Protection Representative will maintain a record of all Personal Data Breaches. This record will contain at least the following information:

13.3.7.1. the facts relating to each Personal Data Breach including the nature of the breach, e.g. paper record lost away from the office, the numbers affected and the types of data affected such as email addresses or customer account details including bank account numbers;

13.3.7.2. the name and contact details of our Data Protection Representative (or other contact point where more information on the Personal Data Breach can be obtained);

13.3.7.3. the effects of the Personal Data Breach (including on the affected Data Subjects) e.g. loss of special category or high risk information including bank account or medical information; and

13.3.7.4. the remedial action taken e.g. advising Data Subjects to reset passwords,

and will be recorded in the format of the data breach log set out in Appendix 6. The ICO or other relevant supervisory authority is entitled to request a copy of our data breach log to verify our compliance with the GDPR. It is therefore vital that you provide as much information as possible, as quickly as possible, about a Personal Data Breach that you become aware of to the Data Protection Representative and that we keep the data breach log up to date.

13.4. What information is required when reporting a Personal Data Breach to the ICO or relevant supervisory authority?

13.4.1. In order to ensure that we can deal with the Personal Data Breach in the appropriate manner, it is essential that accurate and complete information about the breach is provided to us.

13.4.2. You should fill in Part 1 of the Security Breach Incident Form set out in Appendix 3 below and pass the completed form to the Data Protection Representative **without delay**. You need to try to remember or describe, to the best of your knowledge, the circumstances of the Personal Data Breach, including the quantity of data concerned and the nature of the data, whether or not the information lost or destroyed or wrongly processed is special category personal data, high risk data or is particularly important. Special category personal data is defined in Appendix 1. High risk data includes bank account details, passport numbers, driving licence details and national insurance numbers.

13.4.3. The surrounding circumstances as to how the breach occurred may be very important. You should consider the following and be ready to provide this information to the Data Protection Representative when reporting the breach:

13.4.3.1. when the Personal Data Breach occurred (this will be particularly relevant if the Personal Data Breach involves illegal activity);

13.4.3.2. how the data was stored including any relevant security measures relating to the method of storage (for example, paper records in a file or electronic records on a laptop);

13.4.3.3. who was responsible for the data at the time of the Personal Data Breach;

13.4.3.4. whether a third party processor was involved; and

13.4.3.5. how the Personal Data Breach occurred (for example, was the data misplaced or stolen).

13.4.4. If the data was stored on an employee's own device such as a memory stick, laptop or some other mobile device, details of any protection on the device, such as encryption or passwords, should also be noted. Please also see section 20 – BYOD

13.4.5. If a third party processor is involved in processing any personal data which forms part of the Personal Data Breach, that processor should be asked to provide all reasonable assistance and cooperation in dealing with and remedying any Personal Data Breach. Under the GDPR they have a legal obligation to assist.

13.5. Notifying the Personal Data Breach to others

13.5.1. You must **immediately** inform the Data Protection Representative of any Personal Data Breaches, regardless of whether you consider that it does not constitute a risk to the rights and freedoms of a Data Subject.

13.5.2. We will consider notifying the following parties of the Personal Data Breach:

13.5.2.1. individuals whose data is involved in the Personal Data Breach in order to allow them to take any necessary steps to mitigate their losses. Under the GDPR there is a statutory obligation to notify affected individuals where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of those individuals. The Data Protection Representative shall decide whether any individuals should be notified of the Personal Data Breach. However, please be aware that the ICO can require us to notify individuals if we have failed to do so, but it believes the Personal Data Breach creates a high risk;

13.5.2.2. outside media;

13.5.2.3. the police If the Personal Data Breach has arisen as a result of illegal behaviour such as theft, hacking or a denial of service attack; and

13.5.2.4. other affected parties.

Any decision to notify affected individuals will be based on the requirements of the GDPR, ICO guidance, whether the Personal Data Breach is likely to result in a high risk to that individual and whether or not notification will assist the individual to mitigate his/her loss arising out of the incident. If an individual is notified of a Personal Data Breach, we must notify them without undue delay. We must also notify the Personal Data Breach to an individual if required to do so by the ICO.

13.6. Assessing the risk

13.6.1. Once notified of a potential Personal Data Breach, the Data Protection Representative will appoint a team of individuals to investigate the incident. If the Personal Data Breach is significant, this should consist of at least three individuals. The team is responsible for assessing the risk level of the Personal Data Breach incident and assessing the adverse consequences of the Personal Data Breach to the individuals involved.

13.6.2. In the context of assessing the risk which the Personal Data Breach represents, the question that should be considered is what could a third party do with the information? For example, the risk to individuals will be high where bank account details have been lost or sensitive personal data is concerned.

13.6.3. Risks should be categorised as:

13.6.3.1. High risk. This means the incident may result in substantial physical, financial or other harm to an individual, substantial financial impact on our business or another entity, or substantial harm to the reputation, mission or interests of H&H Group Plc or another entity;

13.6.3.2. Privacy risk. This means the incident may result in some injury or harm to an individual, a financial impact on our business or another entity, or loss of a tangible asset or resource, or harm to the reputation, mission or interests of H&H Group Plc or another entity; or

13.6.3.3. Low risk. This means the incident is a technical breach of the GDPR but results in no injury or harm to individuals or H&H Group Plc.

13.7. Containment and recovery

13.7.1. Consideration should be given as to whether there is anything that can be done to mitigate the loss (for example, whether any of the data can be recovered).

13.7.2. We will appoint a team of individuals to work on containing the Personal Data Breach if applicable. The team should be given clear instructions as to what their tasks are (for example, they may be instructed to close a weakness in the IT system through which data has been released).

13.7.3. Consideration should be given as to whether there is anything we can do to limit the damage (for example, utilising back up records to restore the data that is the subject of the Personal Data Breach or promptly notifying individuals affected so they can take measures to reduce the impact of the Personal Data Breach).

13.8. Reviewing the response

13.8.1. Once the Personal Data Breach has been dealt with, we will appoint a team of individuals to consider and evaluate the response. Consideration should be given to:

13.8.1.1. the speed of the response;

13.8.1.2. the adequacy of the response;

13.8.1.3. whether any further training is required for staff;

13.8.1.4. whether any procedures or processes need to be amended; and

13.8.1.5. whether any current policies should be amended in light of the Personal Data Breach.

13.9. If applicable, the results of any review should be communicated to members of staff.

14. Rights of a Data Subject

14.1. We must put in place processes to enable data subject to exercise their legal rights.

14.2. We must provide information requested by a Data Subject pursuant to their rights under the GDPR without undue delay and, in any event, within one month of receipt of a request. This period may be extended by a further two months, if for example there are a number of requests made or a request is particularly complex. **If an employee receives any request from a Data Subject concerning their personal data, they must notify the Data Protection Representative immediately**.

14.3. A Data Subject has the following rights under the GDPR:

14.3.1. A right of access to their personal data and certain other information (see section 15 below for further information);

14.3.2. A right to have any personal data which we hold which is inaccurate rectified;

14.3.3. A right to have incomplete personal data completed (which may include a Data Subject providing a supplementary statement);

14.3.4. In certain circumstances, a right to have personal data concerning them erased, including where the personal data is no longer necessary for the purposes for which it was collected or processed , or if the personal data has been unlawfully processed (see section 14.8);

14.3.5. In certain circumstances, a right for the processing of their personal data to be restricted, including where a data subject contests the accuracy of the personal data held about them, or if the processing of their personal data is unlawful, but the Data Subject does not request that their personal data be erased (see section 14.12);

14.3.6. In certain circumstances, the right to receive the personal data that the Data Subject has provided him or herself, in a portable format that can be transmitted to another data controller without hindrance (see section 14.15;

14.3.7. The right to object to certain types of processing, including profiling and processing for direct marketing purposes; and

14.3.8. In certain circumstances, the right not to be subject to a decision which is based solely on automated processing and which produces a legal effect which significantly affects the Data Subject, for example, when we make a processing decision based on an individual's age or on the postcode in which they live.

14.4. If a Data Subject requests that their personal data be rectified (see 14.3.2 and 14.3.3 above), be erased (see 14.3.4 above) or its processing be restricted (see 14.3.5 above), we must ensure that this is communicated to each recipient of that Data Subject's personal data (unless this would prove impossible or would involve disproportionate effort). If we are unable to communicate this to each recipient, certain recipients of a Data Subject's personal data will not be aware of the rights that a Data Subject has exercised in respect of their personal data, which for example, might mean that a recipient is unaware of a Data Subject's updated and correct personal data. If a Data Subject requests, we must inform the Data Subject about the recipients of their personal data.

<u>The right to have any inaccurate personal data which we hold rectified or incomplete data that we hold completed</u>

14.5. A Data Subject has the right to obtain, without undue delay, the rectification of inaccurate personal data relating to them.

14.6. Taking into account the purpose(s) of the processing, a Data Subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement to us.

14.7. We must make every attempt to ensure that personal data which is inaccurate is rectified or securely deleted.

<u>The right to have personal data erased (the 'right to be forgotten')</u>

14.8. A Data Subject has the right to obtain from us the erasure of their personal data without undue delay. We are obliged to erase such personal data without undue delay where any of the following applies:

14.8.1. The personal data is no longer necessary in relation to the purposes for which they were collected or processed;

14.8.2. Where the processing is based on consent and the Data Subject withdraws their consent and there are no other legal grounds for processing that personal data;

14.8.3. The Data Subject objects to the processing of their personal data (e.g. for purposes of profiling or direct marketing) and there are no overriding legitimate grounds for the processing;

14.8.4. The personal data has been unlawfully processed;

14.8.5. The personal data has to be erased for compliance with a legal obligation to which we are subject; or

14.8.6. The personal data has been collected in relation to the offer of information society services.

14.9. If none of the above apply, and we receive a request to erase a Data Subject's personal data, we are not obliged to comply with the request. We are also not obliged to comply with any such request if the processing is necessary for:

14.9.1. exercising the right of freedom of expression and information; or

14.9.2. compliance with a legal obligation which we are subject to; or

14.9.3. the performance of a task carried out in the public interest or in the exercise of official authority which is vested in us; or

14.9.4. reasons of public interest in the area of public health; or

14.9.5. for archiving purposes in the public interest, scientific or historical research purpose or statistical purposes, insofar as the right to have personal data erased is likely to render impossible or seriously impair the objectives of the processing; or

14.9.6. for the establishment, exercise or defence of legal claims.

14.10. If a request is received by a Data Subject for their personal data to be erased, this must be forwarded to the Data Protection Representative immediately, who will determine whether the request should be complied with.

14.11. If we have made personal data public and we are obliged to erase a Data Subject's personal data, we must, taking into account available technology and the cost of its implementation, take reasonable steps (including technical measures) to inform other data controllers who are processing that personal data that a Data Subject has requested the erasure, by such data controllers, of any links to, copies or replicas of that personal data.

<u>The right to restrict processing of personal data</u>

14.12. Our processing of personal data can be restricted where any of the following applies:

14.12.1. If the Data Subject challenges the accuracy of the personal data we hold, we must restrict the processing of that personal data for a period to enable us to verify its accuracy;

14.12.2. The processing is unlawful and the Data Subject does not wish for the personal data to be erased;

14.12.3. We no longer require the personal data for the purposes of processing but the personal data is required by the Data Subject for the establishment, exercise or defence of legal claims; or

14.12.4. If the Data Subject has objected to the processing (e.g. for profiling or direct marketing purposes), we must cease processing whilst we verify whether our legitimate grounds for processing override those of the Data Subject.

14.13. If the processing of personal data has been restricted, we must only process that personal data (with the exception of storing such personal data):

14.13.1. With the Data Subject's consent;

14.13.2. For the establishment, exercise or defence of legal claims;

14.13.3. For the protection of the rights of another natural or legal person; or

14.13.4. For reasons of important public interest.

14.14. If the restriction on processing is lifted, we must inform the Data Subject of this fact beforehand.

The right to data portability

14.15. A Data Subject has the right to receive the personal data that they have provided to us in a structured, commonly used and machine-readable format. A Data Subject should not be hindered in transmitting that personal data from us to another data controller and, wherever technically feasible, the Data Subject has the right to request that we transfer that personal data directly to another data controller. However, this right only applies where:

14.15.1. The processing is based on the consent of the Data Subject or is necessary for the performance of a contract to which the Data Subject is a party; and

14.15.2. The processing is carried out by automated means.

If these conditions are not met, we are not required to comply with such a request.

14.16. We must ensure that the rights and freedoms of other Data Subjects are not adversely affected if a Data Subject requests their personal data in accordance with section 14.15 above. This may include where the personal data includes the personal data of other Data Subjects, who have not consented to the transfer of their personal data to another data controller.

The right to object to processing

14.17. A Data Subject has the right to object, on grounds relating to their particular situation, at any time, to the processing of their personal data which is:

14.17.1. necessary for the performance of a task carried out in the public interest or exercise of official authority vested in us; or

14.17.2. necessary for the purposes of our legitimate interests or those of 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, particularly if the Data Subject is a child).

14.18. We must not process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override the Data Subject's interests, rights and freedoms or the processing is necessary for the establishment, exercise or defence of legal claims.

14.19. A Data Subject can object to processing at any time where their personal data is processed for direct marketing purposes (which includes profiling to the extent it is related to direct marketing). The personal data must no longer be used for such direct marketing purposes.

14.20. The rights referred to in sections 14.17 to 14.19 above must be explicitly brought to the attention of a Data Subject at the time of the first communication with that Data Subject (at the very latest). These rights must be clearly presented to a Data Subject, separately from any other information.

Automated individual decision making (including profiling)

14.21. A Data Subject is entitled not to be subject to decisions based solely on automated processing (including profiling), which produces legal effects concerning them or which significantly affect them. This includes, for example, if a decision is made about the eligibility of a Data Subject for a particular scheme based on their postcode only.

14.22. The right does not apply however if the decision:

14.22.1. Is necessary for us to enter into a contract with the Data Subject;

14.22.2. Is authorised by law which we are subject to (and which sets out suitable safeguards to protect the Data Subject's rights, freedoms and legitimate interests); or

14.22.3. Is based on the Data Subject's explicit consent.

If the decision is necessary for entering into a contract or is based on explicit consent, we must implement suitable measures to safeguard the Data Subject's rights, freedoms and interests, which as a minimum must include:

- The right to obtain human intervention by us;
- The right for the Data Subject to express their point of view; and
- The right to contest the decision.

15. Dealing with Data Subject Access Requests

15.1. What is a Data Subject Access Request?

15.1.1. Data subjects have a right of access to a copy of their personal data and certain other information.

15.1.2. A subject access request is any request from a data subject which indicates that the person wants to know what information is kept about him or her.

15.1.3. If a verbal request for information is received, an employee may ask the Data Subject to put the request in writing, but should still treat the verbal request as a valid request. The time for us to respond to such request will commence once the verbal request has been made.

15.1.4. If an employee receives a verbal request for information, and has reasonable doubts concerning the identity of the person making the request, we may request additional information from the requester to confirm their identity, before responding to that request.

15.1.5. Internal data subject access requests will be treated as being of equal importance to external data subject access requests.

15.1.6. Answering a subject access request can be time consuming. We will ensure we have adequate resources available to answer subject access requests that are made.

15.2. What should an employee do if they receive a Data Subject Access Request?

Employees must pass all data subject access requests to the Data Protection Representative as soon as possible, as a response must be given within one month. Any delay in passing the request to the Data Protection Representative could result in us failing to meet the statutory deadline and result in enforcement action being taken against us.

15.3. Responding to a Data Subject Access Request

15.3.1. It is the Data Protection Representative's responsibility to respond to a data subject access request. Employees should not send a response without the prior written approval of the Data Protection Representative.

15.3.2. Data subject access requests must be complied without undue delay, and in any event, within one calendar month of receipt of the request. This means if we receive the request on the 3 April we will need to provide the information by the 3 May. The period to respond may be extended by a further two months, if the request is complex and/or there are a number of requests.

15.3.3. We may ask the data subject for further information to help us find the data requested. For example, we could ask for the dates an ex-employee was employed by us or at which site they worked. The one month period to respond does not start until this additional information is received from the requester.

15.3.4. Information provided pursuant to a subject access request should be free of charge to the requester, unless we can demonstrate that the request is manifestly unfounded or excessive (e.g. the requester has made repeated requests for information). In these cases, we can charge a reasonable fee to cover our administrative costs of providing such information and taking the action required, or, alternatively, we can refuse to provide the information.

15.3.5. When a data subject access request is received, the individual should be told whether or not their personal data is being processed. If their personal data is being processed, the individual should be provided with access to that personal data and the following information:

15.3.5.1. the purposes of the processing;

15.3.5.2. the categories of personal data concerned;

15.3.5.3. the recipients or categories of recipient to whom the personal data has or will be disclosed (including any countries or organisations outside the EEA);

15.3.5.4. where possible, the period it is envisaged that the personal data will be stored for, or if this is not possible, the criteria used to determine that period;

15.3.5.5. their right to request rectification, erasure or the restriction of the processing of their personal data, or to object to such processing;

15.3.5.6. the right to lodge a complaint with the ICO or relevant supervisory authority;

15.3.5.7. where the data has not been collected from the Data Subject, any available information as to where it was sourced from; and

15.3.5.8. the existence of automated decision making (including profiling), including meaningful information about the logic involved, and the significance and envisaged consequences of such processing to the Data Subject.

15.3.6. We must provide a copy of an individual's personal data that is undergoing processing. If an individual requests more than one copy of their information, we may charge a reasonable fee based on our administrative costs incurred in dealing with such a request.

15.3.7. If a Data Subject makes a subject access request via electronic means, then unless they request otherwise, we shall provide any information to them in a commonly used electronic form (e.g. via secure e-mail).

15.3.8. In responding to data subject access requests we are required to ensure information relating to an individual, other than the data subject who is making the request, is not disclosed unless:

15.3.8.1. the other individual has consented to such disclosure, in which case written proof of this should be obtained and kept; or

15.3.8.2. it is reasonable in all the circumstances to comply with such request without any consent. This may be the case if the information is already available to the public, for example.

15.3.9. In considering whether it is reasonable to comply with the request, we will consider:

15.3.9.1. any confidentiality owed to the other individual either because we said this information would be kept confidential, or because of the particular circumstances it was disclosed in, or because of the nature of the information;

15.3.9.2. the steps taken to get consent;

15.3.9.3. if the individual concerned can give consent; and

15.3.9.4. any express refusal by such individual to give consent.

15.3.10. A subject access request entitles the data subject to information which contains their personal data. It does not entitle the data subject to all word documents, e-mails etc. which they were copied in on, or which relate to work or projects they were involved in. Where a document contains personal data but also information about other third parties which should not be disclosed in accordance with the considerations set out in section 15.3.9, or contains information which is not personal data, then the document can be provided to the applicant with the information which is not their personal data redacted (blacked out) in the document.

15.3.11. All personal data shall be stored at all times by employees in paper and electronic filing systems which enable us to provide a data subject with details of such personal data promptly and in any event within the time period provided for by the GDPR, see section 12 (*Handling and Storing Personal Data and Data Security*).

15.4. Requests for access to special categories of personal data

15.4.1. All requests by external bodies, agencies or individuals for access to special categories of personal data shall be processed by the Data Protection Representative.

15.4.2. All such requests shall be recorded by such persons in an appropriate system.

15.4.3. The record should state who made the request, when they made it, what the request was and to whom it related.

16. **Employee Personal Data**

16.1. In the course of recruitment and employment we will collect, retain and process information consisting of personal data including special categories of personal data about employees. We must provide employees with a fair processing notice containing the information set out in paragraphs 11.2.1 to 11.2.12 when processing their personal data.

16.2. All employment records, including application forms, interview notes, sickness notes, annual leave records, promotion and appraisal notes, training records, disciplinary and dismissal notes and reports, references (whether confidential or

otherwise and whether given or received) and general personnel file notes must be processed in accordance with the GDPR.

16.3. Personnel records and all written information regarding an employee, including appraisal, career progression and discussions regarding salary should be set out in a manner which contemplates that it may be disclosable as personal data under the GDPR. All records should therefore be clear and fair and, where opinions are expressed, these should be shown to be such.

16.4. The information we hold for the above purposes will be retained in accordance with our *Document Retention Policy*. The purposes for which we hold any information about the employee after the end of employment are for use solely for any residual employment related matters including (but not limited to) the provision of job references, processing applications for re-employment, matters relating to retirement benefits, for dealing with litigation and allowing us to fulfil contractual or statutory obligations.

16.5. Where employee records are maintained for organisational analysis, we will take care to ensure that only that personal data is kept which is necessary to satisfy the purpose for which it is kept. Where possible, such data should be anonymised.

16.6. Where documents are destroyed pursuant to the time periods set out in the *Document Retention Policy*, we shall follow the procedure for destruction set out in section 12.5.5.

16.7. All disciplinary actions, commentary, reports and any reports relating to a dismissal of an individual shall be written in a manner which is fair and accurate.

16.8. All employee records shall be regularly reviewed to ensure that they are accurate, not excessive, up to date and adequate for their purpose. If we believe that any part of an employee's records is inaccurate and/or not-up-to date, we shall notify the employee and request that they confirm the accurate and up-to-date details.

16.9. Use of personal data in recruitment

16.9.1. All recruitment advertisements must contain information which enables applicants to identify that they are applying to H&H Group PLC or a group company.

16.9.2. The interview notes of all applications should be written in consideration that these will amount to personal data under the GDPR. All interview notes should therefore be a fair and accurate representation of the interview. Any opinions expressed should be included in a manner which contemplates that they may be disclosable at a later date.

16.9.3. Where an individual candidate is interviewed but we wish to offer the individual employment other than in the post which the individual has applied for, care must be taken to ensure that the individual has consented to the data being used for this purpose. Candidate details must not be shared with other H&H Group companies unless specific permission has been obtained from the candidate to so do.

16.9.4. Any decision to shortlist candidates, where such decision making is made in writing, should be done in a manner which is fair and lawful.

16.9.5. We will retain information on non-recruited candidates for a period of 6 months after a particular job has been awarded to the successful candidate. After that time, such information should be safely and securely deleted unless we have express permission from a candidate to retain their information.

17. **Customer/Client/Supplier Data and Retention**

17.1. Our customer/client data and certain of our suppliers' data and other data we hold, has the potential to be personal data covered by the GDPR ("**Non-Employee Personal Data**"). A fair processing notice containing the information set out in sections 11.2.1 to 11.2.12 should be made available to all customers/clients/suppliers.

17.2. We shall retain all Non-Employee Personal Data in accordance with our Data Retention Policy and in any event for the minimum periods required by law. Certain documents such as accounting, tax and employment records have specific retention periods. The destruction of other records may, in the context of litigation, be regarded unfavourably by the courts.

17.3. All Non-Employee Personal Data must be processed in accordance with the GDPR and this Framework.

17.4. We shall arrange for all Non-Employee Personal Data personal data records to be regularly reviewed to ensure that they are accurate, not excessive, up to date and adequate for their purposes. If we believe that any part of Non-Employee Personal Data is inaccurate and/or not-up-to date, we shall notify the relevant person and request that they confirm their accurate and up-to-date details.

17.5. Non-Employee Personal Data shall be kept for at least the periods set out in the document retention policy. These are the minimum retention periods. Information may be kept longer than these periods at the discretion of the Data Protection Representative where retention can be justified, provided that such personal data is not kept longer than is necessary for the purpose for which the data was collected.

17.6. Where documents are destroyed pursuant to the time periods set out in the document retention policy, we shall follow the procedure for destruction set out in section 12.5.5.

18. **Use of CCTV**

18.1. CCTV systems process personal data. CCTV processing is intrusive by its nature and where public areas are monitored, specific concerns may be raised under the GDPR. We will ensure that all data recorded by such systems is processed in accordance with this Framework.

18.2. We will keep a record of all CCTV systems we operate. The record will contain:

18.2.1. what cameras are kept and where;

18.2.2. the purpose for the CCTV system. This should include an assessment of the process and the reasons for installation of the scheme; and

18.2.3. confirmation that the CCTV system has been notified to the ICO.

18.3. CCTV equipment should be sited so that it only records that information which is necessary for the purpose of the scheme (i.e. it should not capture images of people not visiting H&H Group premises. Care should be taken to ensure that images are not taken of public or domestic areas, or if they are, that this is restricted in so far as possible. Where the CCTV system records public areas and an outside contractor is used, we shall carry out an impact assessment (see section 7.11 above) and sufficient due diligence to ensure the contractor has appropriate licensing in place (if needed).

18.4. CCTV equipment should only be operated by specified individuals who have been trained appropriately. CCTV images contain personal data and should only be processed by us in accordance with the GDPR. CCTV images must not be copied or circulated within our organisation unless the Data Protection Representative or Chief Executive has provided written permission.

18.5. All zones covered by CCTV should have signs displayed indicating that individuals are entering a CCTV zone. Such signs should be visible and legible.

18.6. The signs should:

18.6.1. include our name;

18.6.2. include the purpose of the scheme (see below);

18.6.3. include who to contact about the scheme; and

18.6.4. be an appropriate size depending on the context, for example, whether they are viewed from a distance.

For example, a sign could say "*Images are monitored for security, crime prevention and public safety. Please contact [ ] on [insert telephone number] for more information.*"

18.7. CCTV must not be used for covert surveillance without the permission of the Data Protection Representative. Covert surveillance must only be used where there is clear evidence of illegal activity taking place and after consultation with the police, if necessary or other relevant enforcement bodies.

18.8. CCTV images must not be retained longer than necessary.

18.9. If a subject access request is received, consideration should be given as to whether images of third parties also included should be obscured. This will be necessary if providing the image would unfairly intrude on the third party's privacy.

18.10. Except for law enforcement bodies and pursuant to subject access requests, images should not be provided to third parties.

18.11. We will check the system regularly to ensure no faults develop or the image quality decreases.

18.12. If we are considering installing a new CCTV system or using an existing CCTV system for a new purpose, we must carry out a Data Protection Impact Assessment.

19. **Home Working and Working Away from the Office**

19.1. During the course of a person's employment with us, there may be times when they will work away from our offices either at home or whilst travelling ("**Home Working**"). Whilst travelling, employees must either use a work laptop or device. Employees must seek permission to work from home unless they are doing so with a H&H Group laptop or mobile device. Where an employee seeks permission to work from home we will need to consider the following activity areas:

19.1.1. information handling - this includes handling data on home pc's, laptops, tablets, smart phones, mobile devices and removable media as well as paper files;

19.1.2. use of services - remote access to our IT system and services; and

19.1.3. systems - managing personal computers and other devices (e.g. to ensure that viruses are not introduced).

19.2. Use of our facilities (e.g. laptops and remote services) when Home Working is for an employee's own work-related use, and such facilities are provided only for authorised purposes. Employees have a responsibility to ensure that other people do not have access to our systems, facilities and services, confidential information, personal data or sensitive personal data (the "**Information**").

19.3. Any loss of Information should be reported in accordance with section 13 (*Personal Data Breach, Notification and Reporting*) of this Framework.

19.4. Employees must keep all Information secure when in transit between locations, for example, they should never leave a laptop or work papers unattended in a public place. When an employee has finished work they should shut down their computer or laptop and put away any papers they have used in a secure place, even if they are at home. When flying with a laptop, it must be kept in hand luggage.

19.5. You should avoid taking Information home whenever possible. Where this cannot be avoided, you should adopt security measures appropriate to the nature of the data.

19.6. In order to ensure compliance with the six data protection principles, employees must keep work related information and files separate from their personal files and when the information is in paper form, preferably in a lockable filing cabinet. Where possible, Home Working should be carried out in a designated area in an employee's home. For example, where an employee lives in a home with individuals who are not members of their family or their children, they should avoid working in a communal part of the home, such as a lounge or kitchen.

19.7. When Home Working, you must not use your own IT equipment to process the Organisation's data.

20. **BYOD**

20.1. Devices

20.1.1. This section applies to the use of smartphones, mobile phones, PDAs, tablets, laptop or notebook computers including any accompanying

software or hardware ("**Device"**) for business purposes. Employees must not use their own Device for work purposes except as set out in this section. This section applies to use of the Device both during and outside office hours and whether or not an employee uses the Device at their normal place of work.

20.1.2. When an employee accesses our systems they may be able to access data about H&H Group PLC, our group companies, our customers, clients, suppliers and other business connections, including information which may be confidential, private or proprietary ("**Company Data**"). When an employee accesses our systems using a Device, we are exposed to a number of risks, including from the loss or theft of the Device (which could result in unauthorised access to Company Data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a Device) and the loss or unauthorised alteration of Company Data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.

20.2. Connection to our systems

20.2.1. Connectivity of all Devices is centrally managed by our IT support providers, who must approve a Device before it can be connected to our systems. Devices must comply with our IT Security Policy.

20.2.2. We reserve the right to refuse or remove permission for an employee's Device to connect with our systems. Our IT support provider will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a Device is being or could be used in a way that puts, or could put, us, our staff, our business connections, our systems, or our corporate information at risk or that may otherwise breach this Framework.

20.2.3. In order to access our systems it may be necessary for our IT support provider to install software applications on an employee's Device. If an employee removes any such software, their access to our systems will be disabled.

20.3. Monitoring content

20.3.1. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a Device (collectively referred to as "**content**" in this Framework) during the course of business or on our behalf is our property insofar as it is created by us or on our behalf, regardless of who owns the Device.

20.3.2. We reserve the right to monitor, intercept, review and erase, without further notice, all content on the Device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing,

retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the Device as well as keystroke capturing and other network monitoring technologies, whether or not the Device is in an employee's possession.

20.3.3. It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Employees should have no expectation of privacy in any data on the Device and are advised not to use our systems for any matter intended to be kept private or confidential.

20.3.4. Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law, for legitimate business purposes, including, without limitation, in order to:

20.3.4.1. prevent misuse of the Device and protect Company Data;

20.3.4.2. ensure compliance with our rules, standards of conduct and policies in force from time to time (including this Framework);

20.3.4.3. monitor performance at work; and

20.3.4.4. ensure that staff members do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.

20.3.5. We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire Device (including personal content) for litigation or investigations.

20.3.6. If an employee has permission to use a Device they confirm their agreement (without further notice or permission) to such monitoring and agree that they have signed an express authority allowing us the right to copy, erase or remotely wipe the entire Device (including any personal data stored on the Device). Employees also agree that they use the Device at their own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any Device, its software or its functionality.

20.4. Security requirements

20.4.1. Employees must comply with IT & communications Policy when using their Device to connect to our systems.

20.4.2. In addition, employees must:

20.4.2.1. at all times, use their best efforts to physically secure the Device against loss, theft or use by persons who we have not authorised to use the Device. They must secure the Device whether or not it is in use and whether or not it is being carried by an employee. This includes,

but is not limited to, passwords, encryption, and physical control of the Device;

20.4.2.2. install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the Device and secure its data, including providing us with any necessary passwords;

20.4.2.3. comply with our Device configuration requirements;

20.4.2.4. protect the Device with a pin number or password, and keep that pin number or password secure at all times. If the confidentiality of a pin number or password is compromised, you must change it immediately. The use of pin numbers and passwords should not create an expectation of privacy by you in the Device;

20.4.2.5. maintain the Device's original operating system and keep it current with security patches and updates;

20.4.2.6. not download and install software to the Device unless explicitly authorised by us.

20.4.2.7. not alter the security settings of the Device without our consent;

20.4.2.8. prohibit use of the Device by anyone not authorised by us, including your family, friends and business associates;

20.4.2.9. not download or transfer any Company Data to the Device, for example via e-mail attachments, unless specifically authorised to do so. Staff must immediately erase any such information that is inadvertently downloaded to the Device;

20.4.2.10. not backup the Device locally or to cloud-based storage or services where that might result in the backup or storage of Company Data. Any such backups inadvertently created must be deleted immediately;

20.4.2.11. not use a Device to capture images, video, or audio, whether native to the Device or through third-party applications, within the workplace;

20.4.2.12. where we have permitted you to store Company Data on the Device, ensure that the Company Data is encrypted using appropriate encryption technologies approved our IT support provider.

20.4.2.13. not use the Device as a mobile hot-spot without our consent.

20.4.3. We reserve the right, without further notice or permission, to inspect an employee's Device and access data and applications on it, and

remotely review, copy, disclose, wipe or otherwise use some or all of the Company Data on it for legitimate business purposes, which include (without limitation) enabling us to:

20.4.3.1. inspect the Device for use of unauthorised applications or software;

20.4.3.2. inspect any Company Data stored on the Device or on backup or cloud-based storage applications and prevent misuse of the Device and protect our Company Data;

20.4.3.3. investigate or resolve any security incident or unauthorised use of our systems;

20.4.3.4. conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and

20.4.3.5. ensure compliance with our rules, standards of conduct and policies in force from time to time (including this Framework).

20.4.4. Employees must co-operate with us to enable such inspection, access and review, including providing any passwords or pin numbers necessary to access the Device or relevant applications.

20.4.5. If we discover or reasonably suspect that there has been a breach of this section 20, we shall immediately remove access to our systems and, where appropriate, remove any Company Data from the Device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from our Company Data in all circumstances. Employees should therefore regularly backup any personal data contained on the Device.

20.4.6. By using a Device for business purposes, employees consent to us, without further notice or permission, inspecting a Device and applications used on it, and remotely reviewing, copying, disclosing, wiping or otherwise using some or all of the data on or from a Device for the legitimate business purposes set out above.

20.4.7. We will not track any personal Devices via GPS or location based Wi-Fi without an employee's or the Device owner's permission.

20.5. Lost or stolen Devices and unauthorised access

20.5.1. In the event of a lost or stolen Device, or where a staff member believes that a Device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to their line manager and the IT support provider immediately.

20.5.2. Appropriate steps will be taken to ensure that Company Data on or accessible from the Device is secured, including remote wiping of the Device where appropriate. The remote wipe will destroy all Company Data on the Device (including Company Data contained in a work e-

mail account, even if such e-mails are personal in nature). Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such data from Company Data in all circumstances. Employees should therefore regularly backup all personal data stored on the Device.

20.6. Procedure on termination of employment

On an employee's last day of work, or their last day before commencing a period of garden leave, all Company Data (including work e-mails), and any software applications provided by us for business purposes, will be removed from the Device. If this cannot be achieved remotely, the Device must be submitted to [the IT Department] for wiping and software removal. Employees must provide all necessary co-operation and assistance in relation to this process. If an employee does not provide the Device to us and it can be wiped remotely, we reserve the right to remotely wipe it and remove software.

20.7. Personal data

We shall use reasonable endeavours not to access, copy or use any personal data held on the Device, unless absolutely necessary. If such access or copying occurs inadvertently, we shall delete any and all such personal data as soon as it comes to our attention. This limitation does not apply to personal data which is also Company Data (including personal e-mails sent or received using our e-mail system). For this reason, employees are encouraged not to use work e-mail for personal purposes.

20.8. Appropriate use

20.8.1. Before using a Device under this Framework for the first time an employee must erase all information and software related to any previous employment. Employees must confirm to us that this has been done if asked to do so.

20.8.2. Employees should never access or use our systems or Company Data through a Device in a way that breaches any of our other policies.

20.8.3. Employees must not talk, text, e-mail or otherwise use a Device while operating a vehicle for business purposes. Employees must comply with any applicable law concerning the use of Devices in vehicles. For their own safety and the safety of others, employees must not use their Device while operating vehicles of any kind.

20.9. Technical support

We do not provide technical support for Devices. If an employee uses a Device for business purposes they are responsible for any repairs, maintenance or replacement costs and services.

20.10. Costs and reimbursements

Employees must pay for their own Device costs under this Framework, including but not limited to voice and data usage charges and any purchase and repair costs. By using a Device for business purposes, employees acknowledge that they

alone are responsible for all costs associated with the Device and that they understand that their business usage of the Device may increase their voice and data usage charges.

21. **Third Party Requests for Data**

21.1. Various persons can legitimately ask for access to personal data held by us. The data subject can ask for his/her personal data by way of a subject access request (see section 14). Additionally a spouse, parent or guardian, solicitor or other party may have or have been granted authority by the individual to ask for personal data. If someone, other than the data subject, claims to have such a right you need to make sure that this authority is valid. You should check any authority granted to make sure it is genuine. In addition, certain third parties can request information under the exemptions set out in the GDPR. This may include where the information is required for matters relating to national security, national defence, public security, the prevention, investigation, detection or prosecution of criminal offences;

21.2. If we receive a request under the GDPR we must first establish the authority requesting the information has the right to use the relevant part of the GDPR. The police have this right as do many government departments. If in doubt, ask the authority to quote the piece of legislation they are relying on for you to provide the information to them.

21.3. The police and other authorities may write to organisations requesting information but it is important we understand the limitations of such requests as they do not create an automatic requirement on us to provide the information. There are limitations to these rights. In the event that any request is made for information by a third party, please contact the Data Protection Representative.

21.4. The GDPR allows the police and other authorities such as the Department for Work and Pensions Benefit Fraud section which have powers to prosecute, to gather data from organisations which is unavailable elsewhere, such as the address and contact details of employees and ex-employees.

21.5. Where we are required to provide information to the police or other authorities, the GDPR exempts us from various requirements, such as the obligation to tell individuals their data is being processed, as this could, for example, tip them off that they are being investigated.

21.6. However, even if the GDPR allows us to provide information to the police or other authorities, we still need a valid processing condition in place. If the data requested includes special category personal data, the circumstances in which it can be released will be more limited. Relevant processing conditions under the GDPR may include where it is pursuant to a legal obligation (such as where there is statutory obligation to assist in an investigation) or where the prosecuting authority has a warrant. Where this is the case, the information must be provided.

21.7. When considering requests:

21.7.1. We must ensure that we properly identify the person requesting the information. If the request is made by phone ask for a written request to be submitted from an official email address or on official letter headed paper.

21.7.2. We must consider whether a refusal to provide the information requested will impede any investigation.

21.7.3. We should provide the minimum information required to fulfil the request (unless the circumstances of the investigation justify greater disclosure (such as in a serious criminal investigation (particularly where there is a real danger to the public or an individual)).

21.8. If a third party seeks information under the GDPR, the Data Protection Representative must be consulted, who will verify whether or not such a request needs to be complied with.

22. **Frequently asked questions**

Q: What should an employee do if they receive a subject access request?

A: Under no circumstances should they respond to it themselves. All subject access requests should be sent to the Data Protection Representative. The Data Protection Representative will send the individual a data subject access request form.

Q: Can we charge someone who makes a subject access request?

A: In most cases, we must respond to a subject access request and provide the information requested free of charge. However, in certain circumstances, we may be able to charge a reasonable fee, taking into account the administrative costs of providing the information. Employees should contact the Data Protection Representative if they receive a subject access request.

Q: If someone asks us to delete all of the personal we hold about them, do we have to comply with this request?

A: This may depend on what we require the personal data for. If, for example, the personal data is no longer necessary for the purposes for which it was collected or processed, or if the personal data has been unlawfully processed, then we must comply with the request. If an employee receives any such request, they should notify the Data Protection Representative.

Q: Can an individual get access to all data which mentions or refers to them when they make a subject access request?

A: No. If releasing the personal data would adversely affect the rights and freedoms of others (for example, if a document refers to a third party's personal data), then we can limit the information which we provide, for example, by redacting any references to third party personal data. If releasing personal data would, for example, disclose trade secrets, or affect intellectual property rights, we can again limit the information which we provide to the individual.

If we process a large quantity of information about an individual, we are entitled to ask the individual, before delivering that information, to specify the information or processing activities to which their request relates.

Q: What should an employee do if they think they have lost some personal data or become aware someone else has lost some data (for example the loss of a laptop)?

A: Report this **immediately** to the Data Protection Representative using a Security Breach Incident Form (see Appendix 3 below).

Q: An individual has asked that we provide them with their personal data as they wish to provide this to another organisation. Are we obliged to do so?

A: In certain circumstances, yes. However, this will only apply to information that an individual has provided to us, and not information that has been obtained from other sources.

If we are obliged to comply with such a request, and the individual so requests, we must transmit such information directly to the other organisation, if this is technically feasible.

We must not provide any information which would adversely affect the rights and freedoms of others. For example, any information provided must not disclose the personal data of third parties.

Q: What should an employee do if the employee of a supplier calls over the telephone and asks for details of their personal data?

A:. We should only disclose it if we can be sure of the identity of the caller. Personal data should only be provided to the data subject itself (and not to a third party) unless you have clear proof that the data subject allows the disclosure of data to such third party (such as a spouse or legal representative). If it is not possible to identify the caller using security questions, you should ask the caller to put their request in writing.

Q: If an email is sent to the wrong person, do I need to do anything?

A: Yes. You should notify the **Data Protection Representative** immediately and complete the Security Breach Incident Form at Appendix 3 as comprehensively as possible.

Q: What should an employee do if they realise, or they are told that some of the personal data we hold is not accurate?

A: They should inform the person who has authority to amend the data that it is inaccurate or they should make the amendment themselves, if applicable. However, if an employee knows the data is correct they do not need to alter our record but they should put a note on the record that the data subject disputes this information is correct.

Q: What should an employee do if somebody complains about the way they are using their personal data?

A: They should take details of their complaint including contact details and tell them that we will respond as soon as possible. They should put the information in the Data Protection Complaint Form set out in Appendix 5 below or ask the data subject to submit a completed form. They should then consider the purpose for which the personal data was collected and whether the way we are using the data is in accordance with that purpose.

Q: I can't breach the GDPR just by talking about personal data, can I?

A: The GDPR can be breached if you talk about another person's personal data which is held by you, whether inadvertently or intentionally.