Data Protection - Policy

Date of this Policy	Next Planned Review date
22/04/2024	22/04/2026
Policy Owner	**Policy Director Lead**
Head of Safeguarding and Governance	Director of Quality

Contents

1 Policy Introduction

1.1 Hesley Group's Commitment to Data Protection

At Hesley Group, we understand how crucial it is to keep personal information safe. This commitment goes beyond just following the law; it's a big part of how we do things and the values we believe in. We want to make sure that the details about our employees, the people we help, and their families are private and secure.

1.2 Purpose and scope of the Policy

The purpose of this policy is to explain how Hesley Group takes care of information, how it supports the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation.

We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy applies to all the information Hesley Group deals with, whether it's on paper, on a computer, or special types of information. It also applies to everyone working with us, like staff, temporary workers, freelancers, consultants, and contractors. It doesn't matter what job they do; everyone must follow this policy.

1.3 Our Approach to Data Management

Hesley Groups' handling of personal data is guided by a set of key principles. These include lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality. Each of these principles is embedded in our operational practices and organisational ethos.

1.4 The 10 Data Security Standards

In 2017, the Department of Health and Social Care put in policy that all health and social care providers must follow the 10 Data Security Standards.

These were developed by the National Data Guardian more information about the National Data Guardian can be found here https://www.gov.uk/government/organisations/national-data-guardian

The Data Security Standards are organised under 3 leadership obligations, People, Process and Technology.

People Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.	**Process** Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.	**Technology** Ensure technology is secure and up to date.
1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.	**4.** Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals.	**8.** No unsupported operating systems, software or internet browsers are used within the IT estate.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.	**5**. Processes are reviewed at least annually to identify and improve processes, which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.	**9**. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework. This is reviewed at least annually.
3. All staff complete appropriate annual data security training and pass a mandatory test,	**6.** Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.	**10**. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.
	7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.	

1.5 Personal Data and Privacy Rights

We understand that personal data is important and private. Handling, using, and protecting this data is a big responsibility for us. We respect the privacy rights of everyone whose data we have and are committed to keeping it safe. Hesley Group will be open and clear about how we handle information about all our "data subjects." Further information can be found in our Being Open (Duty of Candour) policy Corp 8.1

2 Policy

2.1 We Will

2.1.1 Regularly review our Data Protection policy and procedures to ensure compliance with the Data Protection Act 2018 (DPR), the General Data Protection Regulation (GDPR) and all other relevant legislation and guidance.

2.1.2 Ensure that informed and explicit consent is obtained where required and is documented in clear, accessible language and in an appropriate format.

2.1.3 As an employee, you may choose not to give us certain data but you should be aware that this may prevent us from complying with our legal obligations and in turn it may affect your employment with Hesley group.

2.1.4 The individuals we support can exercise their right to withdraw consent at any time, further information in relation to this process is available in P&S 2.4 Information Sharing and Confidentiality Policy.

2.1.5 Process personal data lawfully, fairly, and transparently.

2.1.6 Ensure that we have appropriate and robust governance systems are in place to support effective data protection procedures.

2.1.7 Ensure privacy by design by evaluating the appropriateness of data collections and ensuring secure data processing methods.

2.1.8 Uphold the rights of all individuals whose data we process.

2.1.9 Take prompt action in the case of a data breach, informing the relevant authorities and individuals as required by law.

2.1.10 Monitor and audit our data processing activities to ensure compliance with the policy and data protection laws.

2.1.11 Retain responsibility of data transferred to third party by ensuring sufficient security measures are in place to protect personal data, have a written contract establishing what personal data will be processed and for what purpose and, ensuring that a data processing agreement has been signed by both parties.

2.2 The Data Protection Officer (DPO) will

2.2.1 Complete the Data Security & Protection Toolkit (DSPT) annually alongside other key staff members and monitor compliance with the DSPT.

2.2.2 Monitor compliance with the GDPR and the Data Protection Act 2018 and reporting on data protection and compliance with legislation to the executive team as required.

2.2.3 Define our data protection policy and procedures and all related policies, procedures and processes to ensure that sufficient resources are provided to support the policy requirements.

2.2.4 Promote Awareness and Compliance through regular updates in relation to best practice.

2.2.5 Work with the Hesley Group appointed Caldecott Guardian and Senior Information Risk owner (SIRO) to review and monitor Data protection arrangements and practice across the organisation including the completion of Data Protection Impact Assessments (DPIA)

2.2.6 Liaise, if required, with the Information Commissioner's Office (ICO) where required

2.3 <u>The Caldecott Guardian will</u>

2.3.1 Ensure that the personal information of the individuals we support is used legally, ethically and appropriately and that confidentiality is maintained

2.3.2 Provide Leadership and Guidance on complex matters involving confidentiality and information sharing in relation to those we support.

2.3.3 Work with the DPO to ensure that the highest practical standards for handling person – identifiable information are in place and that the need for confidentiality is extended to other individuals including relatives and staff.

2.3.4 Act as the 'conscience of the organisation' in respect of individuals data.

2.3.5 Apply the eight Caldecott Principles wisely, using common sense and an understanding of the Law as required, see section 4.1 below.

2.4 <u>Managers will</u>

2.4.1 Ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles;

2.4.2 Ensure all staff complete and annual training update in relation to Data protection and Data Security that is relevant to their role.

2.4.3 Monitor and support compliance and policy monitoring, guidance and ensuring adherence to data protection standards.

2.4.4 Manage data access and usage, making sure employees only access data they are authorised to as outlined in policy.

2.4.4 Ensure that any identified data breaches are reported in a timely way onto the Ulysses system.

2.4.5 Securely destroy any copies of personal data that you create as set out in the Records Management and Archives Policy, Corp 4.1, and in any event in line with the data protection principles.
Data destruction schedules are contained within the Hesley group Record Keeping and Archives Policy, Corp 4.1.

2.4.6 Not transfer data outside the European Economic Area unless this has been authorised in advance by the Data Protection Officer or Senior Information Risk Officer.

2.5 All staff will

2.5.1 Ensure the security of personal data at all times – whether it's on paper or held electronically. Use strong passwords and always lock your computer/device when you are not using it. Keep personal data in locked cabinets.

2.5.2 Handle data in a manner that respects the privacy and rights of data subjects, ensuring that personal information is processed fairly, lawfully, and transparently.

2.5.3 Adhere to data protection principles by obtaining personal data only for specified, explicit, and legitimate purposes and ensuring that data is adequate, relevant, and limited to what is necessary.

2.5.4 Be responsible for ensuring the accuracy of the personal data you handle. Any inaccuracies in data must be reported and corrected promptly. Refer to Policy Corp 14.1.5; Flow Chart – How To Report A Suspected Data Breach.

2.5.5 Not disclose personal data to anyone outside the organisation without proper authorisation and ensure that such disclosures are in line with data protection laws and this policy.

2.5.6 Securely destroy any copies of personal data that you create as set out in the Records Management and Archives Policy, Corp 4.1, and in any event in line with the data protection principles.

Data destruction schedules are contained within the Hesley group Record Keeping and Archives Policy, Corp 4.1.

2.5.7 Not transfer data outside the European Economic Area unless this has been authorised in advance by the Data Protection Officer or Senior Information Risk Officer.

2.3.8 Keep their own data up-to-date. Hesley group will prompt you to renew it annually but any interim changes should be notified to us as soon as is practical. See Personal Details of New and Existing Employees, Per 2.1.25.

2.3.9 Personal data must not be stored on your own personal devices and printed copies must not be removed from Hesley group premises without specific authorisation (e.g. sharing information with other providers for the benefit of people we support).

2.3.10 Must only access data that you are authorised to do. Such data must then be processed for the reasons set out in this policy and in line with the data protection principles.

2.3.11 Not share personal data with sources outside Hesley group unless authorised to do so, and only when the data has been encrypted or otherwise made secure.

2.3.12 You must not share personal data with anyone who is not authorised to see that personal data and should consider at all times whether there is a way to share data that might disclose less information, for example anonymising (this means there is no means of the author sourcing the subject of the data once anonymised) or pseudonymised (this is a means of reporting on data that appears to have been anonymised but the author can trace the details of data subjects concerned if necessary). Documents can be redacted as an alternative.

2.3.13 Familiarise yourself with this policy, including the content of the data protection Principles and ensure you comply with them.

2.4 <u>People we support and their families will</u>

2.4.1 Know their data protection rights under the Data Protection Act 2018 and UK GDPR. This includes understanding how your data is used and processed by Hesley Group.

2.4.2 Have a responsibility to provide accurate personal data and inform Hesley Group of any changes or inaccuracies. This ensures that the data held about data subjects remains correct and current.

2.4.3 Provide clear consent for the use of personal data, especially in cases involving sensitive information.

2.4.4 Report Concerns and Breaches to the Hesley Group to allow prompt actions.

2.4.5 Respect the privacy and confidentiality of people we support or employees they may come across.

3 Data Protection Principles

Hesley group will process personal data in accordance with the six data protection principles, which are that all personal data will be:

- Processed lawfully, fairly and transparently.
- Collected and processed for specified explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and in date and any inaccurate data rectified or erased without delay.
- With regard to the reasons for processing, not kept for longer than is necessary.
- Processed in a way that ensures appropriate security.

4 The Role of the Caldecott Guardian

The Caldicott Guardian in Hesley Group is the Director of Quality.

They make sure that the personal information about individuals we support is used legally, ethically and appropriately, and that confidentiality is maintained. The Caldicott Guardian provides informed guidance on complex matters involving confidentiality and information sharing. More information about the role of the Caldicott Guardian can be found on The UK Caldicott Guardian Council website, here.

4.1 The Caldicott Principles

The Caldicott Principles are eight principles to ensure people's information is kept confidential and used appropriately.

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where the use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patients and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

5 Lawful Processing

In line with data protection principles, we will only process personal data and "special category data" for the reasons notified to you and in accordance with our obligations. Under the DPA we must have a specified lawful basis for processing your personal data.

Hesley group processes personal data where necessary to manage the employment relationship and the main lawful bases for processing employees' personal data are:

- To comply with our legal obligations (e.g. paying employee's tax or to fulfil our regulatory requirements as an employer of individuals providing Care, Health and Education Services).
- To perform employees' employment contracts with us (e.g. pay our staff according to the rate agreed).
- Because it is necessary for our legitimate interests – e.g. recruiting suitable staff to sustain an effective and safe service.

Where one of these reasons applies, Hesley group may process employees' information without consent. As an employee, you may choose not to give us certain data but you should be aware that this may prevent us from complying with our legal obligations and in turn, it may affect your employment with Hesley group.

Where we process special category data we will only do so where one of the lawful reasons set out above applies and where either:

- The subject has given their explicit consent.
- Processing is necessary under employment law.
- Processing is necessary to protect an employee or another person's vital interests and the subject is unable to give their consent.
- The subject has made the data public.

- Processing is necessary for a legal claim.
- It is necessary for occupational medical reasons or for the assessment of an employee's or prospective employee's capacity to work.

Where we process special category data Hesley group will inform the subject of the reasons for this at the time.

6 Individuals' Rights as "Data Subjects"

All Employees, People Supported and their Families:

- Have the right to be told what personal data Hesley group processes, how the processing takes place and on what basis. We will issue privacy notices to all applicants and employees and to the people we support and their families.
- Have the right to see their own personal data by making a subject access request; see Procedures for Designated Data Processing Managers - Managing Data Subject Access Requests, Corrections and Erasures, Corp 14.1.1.
- Have the right to receive a copy of their personal data and in some circumstances have their personal data transferred to another data controller, usually within one month and without any charge.
- Can correct any inaccuracies in their personal data.
- May ask Hesley group to erase personal data where it is no longer necessary to process it for the purpose it was collected or where it should not have been collected in the first place.
- May object to data processing where Hesley group is relying on legitimate interest and the individual thinks their interests outweigh ours.
- Will be notified if there is a data security breach involving their data that may affect you.
- Have the right not to consent, or to later withdraw their consent to processing where Hesley group were relying on consent as the lawful reason for processing personal data.
- Have the right to complain to the Information Commissioner, contact details on the ICO Website: www.ico.org.uk

7 Subject Access Requests

All Employees, People We Support and their Families have the right to review the information we hold about them. Please note that unless they are a duly appointed legal representative, or the person concerned has capacity and gives consent, family members of people we support will only be able to review their *own* personal data (for example their own names, addresses, date of birth and other relevant information that constitutes personal data or special category data (e.g. about family medical and social history etc.).

Persons who are duly appointed as their relative's representative (e.g. a Court Appointed Deputy (CAD) for Care and Welfare in respect of care records and CAD for Finance and Property in respect of personal money and possessions) may submit subject access on their relative's behalf.

Please also see Information Sharing and Confidentiality Policy and Guidance, P&S 2.4

Hesley group will usually respond to Subject Access Requests within one month.

The month will be calculated in line with ICO guidance. The day of receipt of the Subject Access Request will be counted as day one. For example, this means if the Subject Access

Request is received on the 3 September Hesley group has until 3 October to comply. If there is no corresponding calendar date in the following month, the date for responding will be the last day of the following month.

No charge will usually be made for a response to a Subject Access Request.

If a Subject Access Request is made to a manager from another member of staff it should be forwarded immediately Head of Safeguarding and Governance.

8 Monitoring and Compliance

Hesley Group monitors the use of the company computer systems (including your e-mails, internet use on work computers and devices) it does this to protect other Employees, people supported and their families and duties owed to suppliers and commissioners. Other specific monitoring in place includes the use of Hesley groups' vehicles – please see the Safe Driving Policy, H&S 1.9, and the use of CCTV cameras outside some of our premises.

If any other monitoring is being considered for employees (e.g. drug and alcohol testing) you will be advised of this and given all relevant information, including the lawful basis for processing the data at the time such monitoring is put in place.

In all cases a Data Privacy Impact Assessment (DPIA) will be undertaken before monitoring is put in place. Covert monitoring will only take place exceptionally and where the Privacy Impact Assessment has established there is no less intrusive means of gathering the information.

Hesley Group Policy on the Use of Surveillance in Residential Care Settings, P&S 2.8, describes our approach to monitoring people we support where there is an identified need and lawful basis, whether by audio, electronic or visual links to their property.

9 Recording of Images

Hesley Group has two separate policies on the use of video recordings, audio, clinical and non-clinical purposes for people we support. See Non-Clinical Video, Photography and Audio Recording, P&S 2.3, and Taking and Use of Photographic/Video Images or Audio Recordings for Therapeutic/Clinical Purposes, P&S 2.3C.

Where it is necessary for our purposes of fulfilling an employment contract and other issues such as security and safety (e.g. an employee photograph on an ID Badge) this will be reflected in the privacy notice relating to employee records. If it is felt to be desirable rather than essential, for examples people being included in photographs of key events or learning and development staff being video recorded delivering training sessions, specific detailed consent will be needed. This will need to advise the individual of the purposes of the recording, how we plan to keep it, who will see it, when it will be destroyed and their rights to consent, withdraw consent or deletion. Please see Specific Issue Consent Form – Learning & Development Team, Corp 14.1.2a, Specific Issue Consent Form – Photographic Images - Employees, Corp 14.1.2b.

10 Privacy Notices

10.1 We will let you know what data we collect

Whenever we collect information from you, are provided information about you, or are planning to pass on your information to a third party, we will provide you with a Privacy

Notice giving clear information about how and why your data is being used, where it comes from and where it goes to. This section gives an overview of the data we usually collect and use about you in the course of your relationship with us. As an employer and provider of services, we need to process your information for a range of reasons.

10.2 Data Routinely Collected – Employees

For employees during your recruitment, during your employment with us and following the termination of your employment. We will use this data to decide whether or not to employ you, check that you have the right to work in the UK, decide what salary and terms to offer you, and then administer the ongoing contract between us, for example, managing your performance and conduct at work, making reasonable adjustments if you have a disability, paying you and deducting the right amount of tax and insurance.

- Name and date of birth
- Address and phone number
- ID documents and information about your immigration status
- National Insurance Number and details of tax status
- Information about your previous employment history
- Your qualifications and memberships
- Your job title and place of work
- Information about your contract including your start date, working hours, salary and benefits
- Gender, marital status and details of dependents
- Contact details for emergency contact person
- Information about your performance including appraisal and supervision records
- Details of training received
- Details of any grievances raised or in which you were involved
- Disciplinary records
- Attendance records including details of your access to and from the workplace using the swipe card system
- Images of you from our staff records (required by regulation as proof of ID) and from any Company CCTV systems
- Records of any correspondence between you and Hesley group about your employment including for example any changes to your contract.

The information will be retained as set out in our Records Management and Hesley group Archives Policy, Corp 4.1.

10.3 Data Routinely Collected – People Supported and Their Families

Data Routinely Collected - People Supported and their Families may take place during the pre-admission and assessment process, during the person's stay at Hesley group and following the person's leaving Hesley group. This may include information contained within:

- Support plans
- Assessments
- Daily records
- Mental capacity assessments
- Best interests' decisions
- Personal information relating to history, health and wellbeing

- Records of significant incidents
- Behaviour support records
- Education plans and young people's work

We are required by Regulation to retain personal data securely for fixed periods of time. Please see Records Management and Hesley group Archives Policy, Corp 4.1.

10.4 Data Routinely Collected – Students in Education Setting:

- Name
- DoB
- Family & Social History
- Family Information
- Medical information required by the college
- New starters
- Assessment outcomes
- Progress mapping data
- Educational plans
- Activities in school and off site
- Accidents and injuries
- Behavioral Incidents
- College reports
- Adult safeguarding

College staff records are maintained centrally and come under the Employee section above.

Historic children's services records are retained in line with the policy requirements in place at the time of closure. For further information and access to these records please contact the Head of Safeguarding and Governance.

10.5 National Data Opt-Out

Hesley Group reviews all of our data processing on an annual basis to assess if the national data opt-out applies. This is recorded in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies.

If any data processing falls within scope of the National Data Opt-Out we use MESH (Messaging exchange for social care and health) to check if any of our service users have opted out of their data being used for this purpose.

11 Minutes of meetings

Minutes of Meetings concerning or referring to individuals who use or are referred to use our services, staff and relevant others, e.g. family members, are to be treated in confidence in the same way as any other record maintained by Hesley group. For clarity, the sentence below should be added at the foot of minutes:

"Please note that these minutes are to be treated in the same way as any other confidential records maintained by Hesley group, in accordance with the Data Protection Policy at Corp 14.1 and Hesley group Staff Code of Conduct".

12 Personal information and Data Breach

12.1 Any Employee found to be in breach of this policy may be liable to disciplinary action up to and including, for serious or deliberate breaches, summary dismissal for gross misconduct.

12.2 If a data breach is suspected, you **Must** take action by notifying your manager who will help you to report the breach on the Ulysses system. Refer to Policy Corp 14.1.5; Flow Chart – How To Report A Suspected Data Breach.

12.3 You must also take action to stop the breach getting worse, for example, by:

a) Confirming that an email has been deleted by the recipient following accidental disclosure, or if possible, revoke any further access.

b) Recovering lost paper records or any lost device left in a public place.

c) Changing the access codes to any compromised building.

d) Informing IT in the event of any compromised computer or data access or anything suspicious or untoward on your device, applications or network files & folders.

e) Disconnecting your device from the network and report directly to IT, if you suspect you are being directly targeted in a cyber-attack.

13 Further Information

If you have any questions about Hesley group's Data Protection Policy please contact the Head of Safeguarding and Governance (Data Protection Officer) who is based within the Quality Team.

14 Training Consideration

All employees require annual training about understanding their data protection responsibilities.

Those will specific roles in relation to data protection require specialist training that should be updated on an annual basis.

15 Related Legislation and Guidance

This policy is in place to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

16 Associated Documents, standard forms and letters

16.1 Data protection policy – guidance Data Breaches and Subject Access requests, Corp 14.1.1

16.2 Specific Issue Consent Form – Learning & Development Team, Corp 14.1.2a

16.4 Specific Issue Consent Form – Photographic Images - Employees, Corp 14.1.2b

16.5 Privacy Notice – Employee, Corp 14.1.3b – please note privacy notice for Job applicants is available within the E-ploy recruitment system

16.6 Model Conversation and Record – Verifying the Identity of a Data Subject Corp 14.1.4a

16.7 Model Internal Email Asking Staff to Search their Records Corp 14.1.4b

16.8 Model Letter of Acknowledgement, Corp 14.1.4c

16.9 Model Letter - Obtaining a Valid Subject Access Request (Further Information Required), Corp 14.1.4d

16.10 Model Letter – Obtaining the Opinions of a Third Party (including Referees), Corp 14.1.4e

16.11 Model Letter – Acknowledgement of the Third Party's Consent to Disclose the Information, Corp 14.1.4f

16.12 Model Letter – Acknowledgement of the Consideration of the Third Party's Opinions Regarding Disclosure of the Information and Explanation of Decision Reached, Corp 14.1.4g

16.13 Model Letter – Replying to a Subject Access Request: Providing the Requested Information, Corp 14.1.4h

16.14 Model Letter – Release of Part of the Information, when the Remainder is covered by an Exemption (Excluding References), Corp 14.1.4i

16.15 Model Letter – Replying to a Subject Access Request Explaining Why You Cannot Provide Any of the Requested Information (Excluding References), Corp 14.1.4j

16.16 Model Letter – Replying to a Subject Access Request Explaining Why You Have Only Sent Some of the Requested References, Corp 14.1.4k

16.17 Model Letter – Replying to a Subject Access Request Explaining that only References Received by Hesley group are Liable for Disclosure, Corp 14.1.4l

16.19 Flow Chart – How To Report A Suspected Data Breach, Corp 14.1.5

16.20 Quick Office Audit and Action plan – Data Protection, Corp 14.1.6

17 Other Policy References

17.1 Information Governance in the Hesley group, Corp 2.1

17.2 Records Management and Hesley group Archives, Corp 4.1

17.3 Information Sharing & Confidentiality, P&S 2.4

17.4 Disclosure and Barring Service (DBS) Checks on Potential and Current Employees, Per 2.5

17.5 Personal Details of New and Existing Employees, Per 2.1.25

17.6 Use of Photographic/Video Images or Audio Recordings for Therapeutic/Clinical Purposes, P&S 2.3C

17.7 Safe Driving Policy, H&S 1.9

17.8 Hesley Group Policy on the Use of Surveillance in Residential Care Settings, P&S 2.8

17.9 Acceptable Use of Hesley Group IT Facilities, Fac 5.1

18 Appendices

18.1 Guidance from Regulatory Authorities

- Information Commissioner's Office (ICO) Guidelines
  https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- ICO Code of Practice
  https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/
- Data Protection Act 2018 (HM Government)
  http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf
- The UK Caldicott Guardian Council
  https://www.ukcgc.uk
- GDPR ICO Website Support
  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- National Data Guardian
  https://www.gov.uk/government/organisations/national-data-guardian