Data Protection Policy

COVID-19 NOTICE

During the current emergency there will be times when Hesley Group is asked to share information with the Local Authority and the NHS for reasons of managing public health and safety. Our duty to people employed and supported is to ensure the information is transferred securely and being shared for valid reasons and avoid scams and breaches. The ICO says the following in relation to collecting and sharing information about people's health:

Can I collect information about employees' health?

You have an obligation to protect your employees' health, but that doesn't necessarily mean you need to gather lots of information about them.

It's reasonable to ask people to tell you if they have visited a particular country, or are experiencing COVID-19 symptoms.

You could ask visitors to consider government advice before they decide to come. And you could advise staff to call 111 if they are experiencing symptoms or have visited particular countries. This approach should help you to minimise the information you need to collect.

If that's not enough and you still need to collect specific health data, don't collect more than you need and ensure that any information collected is treated with the appropriate safeguards.

Can I share employees' health information to authorities for public health purposes?

Yes. It's unlikely your organisation will have to share information with authorities about specific individuals, but if it is necessary then data protection law won't stop you from doing so.

Please see the ICO website for more FAQs
https://ico.org.uk/for-organisations/data-protection-and-coronavirus/

1 Policy Introduction

Hesley Group Limited recognises its obligations under the Data Protection Act 2018 (DPA) and in particular the importance of respecting the personal privacy of all its employees, the people we support and their families, as listed below, and the need to build in appropriate safeguards regarding the use of personal data.

Throughout this policy we refer to Employer, Employee and Employment for ease of reading. This policy applies to all employees, agency workers, freelancers, consultants, etc. ("Employees") who work, *may work for, or have previously worked* for Hesley Group.

The DPA also applies in respect of protecting the information of people we support at Hesley Group (children, young people and adults who use, may use *or have previously used* Hesley Group services) and their families.

The policy explains how Hesley Group will hold and process information we have about all these people and their rights as "data subjects". It also explains obligations of employees with regard to data protection during their employment or engagement with Hesley Group.

This policy is not contractual and may be amended at any time. Because of the introduction to the DPA and the General Data Protection Regulations (GDPR) in 2018 this policy is subject to continued development. Changes will be notified as and when they occur to key managers in order that they may update their staff teams.

2 What is Personal Data?

2.1 Personal Data

Personal data is defined as data that relates to a living individual who can be identified from the data and includes any expression of opinion about the individual and any indication of intention in respect of that individual. It does not include data that has been fully anonymised. *NB Anonymisation means there is no means of tracking the data back to its subject. Pseudonymisation means data that protects the identity of an individual by giving them a pseudonym or code, but there is a means in the organisation or elsewhere of tracking the data back to the subject – e.g. employer number.*

Hesley Group holds data about our employees on:

- Our Infonet
- Security records and systems
- Time Keeping records
- Telephone recording or monitoring systems
- CCTV
- E-mail systems
- Electronic (e.g. PeoplePlanner) and paper-based HR files
- Payroll

Hesley Group holds information of people we support and their families on:

- Paper-based and electronic personal support files and daily journals
- Clinical and therapeutic services records
- Multidisciplinary meeting records and other review formats

- Incident and accident/injury databases
- Records of complaints
- Safeguarding records
- Medication records
- Medication error reports
- Deprivation of Liberty spreadsheets
- Record forms of Incidents, Injuries and Accidents
- Referral papers
- Business Development Reports
- E-mail systems

Personal data may be provided by the data subject themselves or by third parties, for example former employers, Local Authorities and CCGs, or may be created during the employer-employee relationship (e.g. supervision records) or during the time a person we support is using Hesley Group services. A summary of the information Hesley Group collects and the reasons for this is set out in Section 11. Specific details of the personal data that Hesley Group processes will be provided within privacy notices.

2.2 Special Category Data and Data Relating to Criminal Offences or Convictions

Special category data is information as to:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical belief
- Trade union membership
- Genetic or biometric data
- The person's health
- Details of sex life
- Sexual orientation
- Offending history/convictions

Hesley Group may collect information from employees in a way that is anonymised so as to monitor the effectiveness of our equal opportunities policies. Where this is the case it will *not* be considered personal data. However, where the information has not been anonymised this will clearly be special category data and treated as such. A significant amount of information that we collect about people we support and on occasion their family members will be categorised as special category data. Details of any special category data that Hesley Group collects and processes about employees or people we support and their families will be explained in detail at the time of collection. Where an individual does not have mental capacity to understand the information this will either be provided to a properly appointed legal representative (e.g. Court Appointed Deputy for Care and Welfare or Property and Finances) or the parent or person/authority with parental responsibility for a child aged under 16 years.

Hesley Group processes personal data relating to criminal convictions to meet our regulatory obligations. Full details are set out in the appropriate Privacy Notice if you are working in regulated activity as part of your role and in our DBS (Disclosure & Barring Service) Policy, Per 2.5.

2.3 What is processing?

Processing means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data. It applies to a comprehensive range of activities including the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

2.4 Privacy by design

Privacy is central to data protection law and, therefore, Hesley Group will investigate the risks to employees and people we support and their families of processing their personal data, minimise those risks, wherever possible (by assessing whether it is appropriate to collect the data in the first place), use appropriate methods to process data and ensure that the processing is secure.

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 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.

5 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 DP 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

6 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 aged 16 years and above 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. Parents of children aged 15 and below may request to see personal data on their child's behalf if the child has capacity and consents, or if the child is considered to lack capacity and it is deemed to be in their interests to share such data.

Please also see Information Sharing and Confidentiality Policy and Guidance, ReS 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 an employee from another member of staff it should be forwarded immediately to the HR Manager. If a Subject Access Request is made about a person we support or a family member it should be forwarded immediately to the Head of Policy and Regulation.

7 Data Security and Employee Obligations

Access to employee data and that of people we support and their families will be restricted to those users with a specific and legitimate business need for the data. **If you are an employee with access to personal data pertaining to other employees or people we support and their families, etc., then you MUST familiarise yourself with this policy, including the content of the data protection principles and ensure you comply with them**

All employees have obligations in regard to handling data at work. As an employee your obligations are specifically:

You must keep your 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.

You must keep all data secure – 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.

You must only access data that you are authorised to do. You must then only process data for the reasons set out in this policy and in line with the data protection principles.

You must 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.*

You must not share personal data with anyone 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 anonymizing (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.

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).

Do 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.

Do not transfer data outside the European Economic Area unless this has been authorised in advance by the HR Manager or Head of Policy & Regulation.

If you receive a subject access request please refer it to:

Employees - the HR Manager or in their absence the Chief Operating Officer.

People We Support and their families - Head of Policy & Regulation. Or the Policy & Regulation Manager.

If you become aware of a possible data security breach however minor it seems at the time please report it to the senior manager on duty at your service, alternatively HR Manager or Head of Policy and Regulation/Policy & Regulation Manager.

If you are ever in doubt as to your obligations please contact the HR Manager or Head of Policy and Regulation/Policy and Regulation Manager for clarification.

8 Monitoring

As an employee of Hesley Group we will monitor your use of the company computer systems (including your e-mails, internet use on work computers and devices) because it needs to do so to protect other Employees, People Supported and their Families and duties owed to suppliers and commissioners. Other specific monitoring includes the use of Hesley Group vehicles – please see the Safe Driving Policy, H&S 1.9, and the use of CCTV cameras outside 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 Privacy Impact Assessment will be undertaken. 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, ReS 2.8, describes our approach to monitoring people we support, 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 – Children and Adults, ReS 2.3, and Taking and Use of Photographic/Video Images or Audio Recordings for Therapeutic/Clinical Purposes, ReS 2.3C. Where it is necessary and essential 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 and Specific Issue Consent Form – Photographic Images - Parental Consent (Children Under 16 Years), Corp 14.1.2c.

10 Where Data is Handled by a Third Party

Where individual's data is transferred to a third party (for example a payroll provider in the case of an employee or medical practitioner in the case of people we support) Hesley Group still retains responsibility for the secure and appropriate use of that data. Consequently, before any individual's data is transferred to a third party Hesley Group will:

- Ensure that the third party has sufficient security measures in place to protect the processing of personal data.
- Have in place a written contract establishing what personal data will be processed and for what purpose.
- Ensure that a data processing agreement has been signed by both parties.

11 Privacy Notices

11.1 We will let you know what data we collect

Whenever we collect information from you, are provided by 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.

11.2 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, 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.

11.3 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 children'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.

11.4 Data Routinely Collected – School Pupils in Education Setting & Their Families: *NB other than for day pupils, some of these will inevitably cross over with the children's homes provision.*

- Name
- DoB
- Family & Social History
- Family Information
- Medical information required by school
- New starters
- Assessment outcomes
- Progress mapping data
- Educational plans
- Activities in school and off site
- Accidents and injuries
- Behavioural Incidents
- School reports
- Child Protection and Safeguarding Children

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

11.5 **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 Breaches of this Policy

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.

13 Further Information

If you have any questions about Hesley Group's Data Protection Policy please contact HR Manager or Head of Policy and Regulation.

Date of this Policy	Next planned review date
22/03/2023	30/06/2023

14 Standard Forms, Letters and Documents

14.1 Procedures for Designated DP Managers - Managing Data Subject Access Requests, Corp 14.1.1

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

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

14.4 Specific Issue Consent Form – Photographic Images - Parental Consent (Children Under 16 Years), Corp 14.1.2c

14.5 Privacy Notice - Job Applicant, Corp 14.1.3a

14.6 Privacy Notice – Employee, Corp 14.1.3b

14.7 Privacy Notice – Child (aged 13-15 years), Corp 14.1.3c

14.8 Privacy Notice – Young Person (aged 16-17 years), Corp 14.1.3d

14.9 Privacy Notice – Adult over 18 years, Corp 14.1.3e

14.10 Model Conversation and Record - Verifying the Identity of a Data Subject, Corp 14.1.4a

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

14.12 Model Letter of Acknowledgement, Corp 14.1.4c

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

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

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

14.16 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

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

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

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

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

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

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

14.23 Data Breach Notification Form, Corp 14.1.6

14.24 Data Breach Risk Assessment Table, Corp 14.1.7

14.25 Briefing No. 1 – Privacy and Personal Data of People We Support, Corp 14.1.8a

14.26 Briefing No. 2 - All Staff – Data Breaches, Corp 14.1.8b

14.27 Briefing No. 3 - Information Requests – Employees/Former Employees, Corp 14.1.8c

14.28 Briefing No. 4 - Data Subject Access Requests – People we Support, Corp 14.1.8d

14.29 Quick Office Audit and Action plan – GDPR, Corp 14.1.9

15 Other Documents to be Referred to

15.1 Information Governance in the Hesley Group, Corp 2.1

15.2 Records Management and Hesley Group Archives, Corp 4.1

15.3 Information Sharing & Confidentiality, ReS 2.4

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

15.5 Personal Details of New and Existing Employees, Per 2.1.25

15.6 Non-Clinical Video, Photography and Audio Recording – Children and Adults, ReS 2.3

15.7 Use of Photographic/Video Images or Audio Recordings for Therapeutic/Clinical Purposes, ReS 2.3C

15.8 Safe Driving Policy, H&S 1.9

15.9 Hesley Group Policy on the Use of Surveillance in Residential Care Settings, ReS 2.8

15.10 Acceptable Use of Hesley Group IT Facilities, Fac 5.1

15.11 Email Policy, Fac 5.4

15.12 Data Protection Act 2018 (HM Government)
http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

15.13 GDPR in Education (DfE Publication)
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

15.14 GDPR ICO Website Support
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/