Policy Number: BMM19

Data Protection and GDPR Policy

Quality Standards

	Legislation	Details
	Regulation 4: The leadership and management standard	The registered person must manage the supported accommodation in accordance with the ethos and outcomes set out in the Statement of Purpose, ensuring all staff comply with their obligations with respect to the handling and storage of personal information, and inform young people of their rights confidentiality and privacy under data protection legislation.
	Regulation 5: The protection standard	The registered person must put arrangements in place to protect young people's safety and security and manage risks. Staff must share relevant information with accommodating authorities for safeguarding purposes and should inform young people of any information sharing and the reasons behind it. The setting's protection policies should reflect requirements of other relevant legislation, including data protection laws.

	Regulation 6: The accommodation standard	The registered person must provide a comfortable and secure living environment where young people's privacy is respected. The registered person must ensure compliance with data protection law, protecting young people's confidentiality and personal data, and informing them of the use of any surveillance or monitoring equipment and its purpose.

Key Principles

	Principle	**How this applies to Data Protection**
	I feel safe and secure where I live and in my wider environment.	Taking steps to ensure young people's personal data is secure and informing them of their rights under data protection law helps them feel safe and secure and that their privacy and confidentiality is respected.
	I have strong, trusting and meaningful relationships within my support system and can rely on the adults around me.	Training staff to adhere to data protection law and inform young people of their rights helps build strong relationships where young people can trust that their information will be kept secure.

This Policy should be read in conjunction with our other Policies on:

- Confidentiality and Privacy
- Records
- Subject Access Requests
- Rights of the Young Person - Access to Their Personal Files & Case Notes
- Access to Records
- Handling Disclosure Information
- Data Breach
- Employee Data Protection
- Whistleblowing
- Safeguarding
- Use of Social Media
- Email and Internet
- Image Capturing
- CCTV and Surveillance
- IT Equipment Disposal

Policy Statement

Policy Aims

This Data Protection and GDPR Policy sets out the values, principles and procedures underpinning Orchard Therapeutic Care Ltd.'s approach to recording, handling, storing, and deleting information about the young people as well as staff and other stakeholders, in a way that upholds discretion, confidentiality and security.

The Policy has been designed to ensure compliance with all relevant guidelines and UK legislation, including the Data Protection Act 2018 and the General Data Protection Regulation.

As a provider of supported accommodation for young people, Orchard Therapeutic Care Ltd recognises the importance of honouring young people's privacy and confidentiality as a vital duty of our position of trust, and this includes protecting their personal information or data, as well as that of their families, visitors, staff, and all relevant others.

In line with its registration under the Data Protection Act 2018, and to comply with the General Data Protection Regulation (GDPR), Orchard Therapeutic Care Ltd understands its accountability for the processing, management, regulation, storage, and retention of all personal data held in the form of manual records and on computers. This Policy defines the arrangements in place within Orchard Therapeutic Care Ltd to ensure compliance with the requirements of the data protection legislation, as applicable to our supported accommodation services.

The Policy applies to all physical and digital records kept by Orchard Therapeutic Care Ltd in relation to young people in the service, their families and other associates whose personal data might be found on their records, all staff and any third parties (agencies and professionals) with whom anyone's personal data might have to be disclosed or shared.

Background

Since the UK withdrew from the European Union (EU), the EU-GDPR is no longer applicable to UK law. As such, the UK has had an "adequacy decision" approved by the EU Commission, meaning it has been judged to have appropriately equivalent data protection laws in place. These laws are called the UK General Data Protection Regulation (UK-GDPR) and they fulfil the same purpose as the EU-GDPR does for countries within the EU.

The UK-GDPR is covered within the Data Protection Act 2018 (DPA), the overarching legislation which governs how personal information is gathered, handled, stored, accessed, shared, and erased in the UK.

This Policy reflects Orchard Therapeutic Care Ltd.'s commitment to following the UK-GDPR and DPA, and will be reviewed alongside any future legislative changes. The UK's "adequacy decision" is set to be reviewed in 2025.

Principles

The core activities of Orchard Therapeutic Care Ltd involve the collection and processing of personal information about. Most of this information originates from the young people using our service in case files, support plans, needs and risk assessments, safeguarding/incident reports, medical records, etc., but some staff data is also recorded such as employment records, rotas and training logs. Personal data can take the form of written/verbal information, images (e.g. CCTV footage, ID photos), or biometric data (e.g. fingerprint scans for entry systems).

All personal details are subject to data protection laws, but some data are considered more sensitive than others. General personal data is any information relating to an individual who is identified or otherwise identifiable, directly or indirectly. Examples of personal data include:

- Date of birth
- ID photo
- Mobile number
- Driver's licence

Sensitive personal data is information about an individual that requires additional protection under the GDPR. Sensitive personal data includes:

- Ethnicity/racial origin
- Religious beliefs
- Physical/mental health
- Gender/sexual identity
- Political affiliations
- Genetic/biometric data

Sensitive data is more strictly controlled than general personal data. Staff are trained in the different types of data needed for particular activities, for example, the development of a young person's support plan. Since it is highly likely that a support plan will include a mixture of sensitive and non-sensitive data, care must be taken to only use the data required, and not more than is absolutely necessary to deliver a high-quality service.

All individuals, including young people and employees, have the right to access all physical and digital records of their personal data. For young people, this is supported by our Confidentiality Policy.

The way in which Orchard Therapeutic Care Ltd manages young people's information will conform to the following general principles:

- Justify the purpose of using private information
- Only request or use data when absolutely necessary
- Use and keep no more data than is required

- Authorise access on a strict need-to-know basis
- Everyone should understand their own responsibilities
- Understand and comply with the law.

All personal data obtained and held by Orchard Therapeutic Care Ltd to carry out its activities as a supported accommodation provider must be:

- obtained fairly and lawfully
- held for specified lawful purposes as an organisation performing a public duty
- processed in recognition of people's data protection rights, described in the UK-GDPR as the right to:
    - be informed of when and what data is recorded, and how it is used
    - have access to their data
    - have records kept accurate, and inaccuracies corrected
    - have data deleted as requested, or if inaccurate or irrelevant)
    - restrict the processing of data to keep it fit for its specified purpose(s)
    - have data sent elsewhere as requested or consented to
    - object to the inclusion of any data (e.g. if considered irrelevant)
    - regulate any automated decision-making and profiling of their data.
- adequate, relevant and not excessive in relation to the specified purpose of its use
- kept accurate and up to date, using agreed means of recording (physical or digital)

- kept for no longer than necessary for its specified purpose (e.g. in line with agreed retention protocols for each type of record)
- protected from unauthorised use, loss or damage with clear procedures for investigating data security breaches
- transferred in compliance with the UK-GDPR procedures for international transfer of personal data (where relevant).

In line with the DPA and UK-GDPR, Orchard Therapeutic Care Ltd has a nominated data controller and data protection officer responsible for the safekeeping and safeguarding of all personal data held by the organisation.

Procedures

Orchard Therapeutic Care Ltd will keep full, accurate, up-to-date records on service users, staff and other stakeholders, and all other aspects of the running of the service, in line with proper procedures of data protection, confidentiality, secure storage and authorised access.

Orchard Therapeutic Care Ltd understands that all records required for the protection of young people and for the effective and efficient running of the supported accommodation should be collected, maintained and kept according to the DPA and UK-GDPR.

Our procedures fully endorse and adhere to the six principles of data protection set out in Article 5 of the GDPR:

1. Data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that any personal data that are inaccurate, with regard to the purposes for which they are processed, are erased or rectified without delay.

5. Data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

6. Data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful access or processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Orchard Therapeutic Care Ltd is legally required to follow the above principles whenever processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Orchard Therapeutic Care Ltd will:

- observe fully the conditions regarding the fair collection and use of personal information, including obtaining informed consent
- specify the purposes for which information is kept and used
- collect and process appropriate information only to the extent that is needed to fulfil our operational needs or legal obligations
- assure the quality and accuracy of information we keep and use
- ensure information is held for no longer than necessary
- ensure that the data protection rights of people whose information is held can be fully exercised under the GDPR (see above)
- take appropriate technical and organisational security measures to safeguard personal information
- declare and honour the data subject's right to appeal to the Information Commissioner's Office if an agreement cannot be reached in a dispute over their personal data

- ensure personal information is not transferred internationally without suitable safeguarding measures
- carry out risk assessments as part of our reviewing activities to identify any vulnerabilities in our data handling and processing, and make arrangements to reduce the risks of mishandling and potential data breaches, including impact assessments of use and misuse of personal data in and by the organisation
- implement appropriate mechanisms for detecting, reporting and investigating suspected or emergent data breaches, including security breaches, and report to the Information Commissioner any significant breaches that cause significant harm to the affected individuals, and understand the possible consequences (e.g. a fine)
- appoint a data controller and data protection officer responsible for the safekeeping and safeguarding of all personal data by Orchard Therapeutic Care Ltd.

Orchard Therapeutic Care Ltd is fully committed to upholding the legal principles of data protection as defined by the ICO. In particular:

- Young people will be kept informed of the who, why, when, where and how ("WWWWH") in relation to the processing of their data.
- Everybody whose data will be held or used by Orchard Therapeutic Care Ltd will be provided with a Privacy Notice identifying the circumstances under which any data they volunteer is collected and processed and outlining the requirement for written consent to data collection. The following will be considered when writing the Privacy Notice:
    - The information being collected
    - Who will collect the information
    - The means of collection (e.g. written, images, audio recording; physical, digital/online)

- The purpose of collecting the information
- How the information will be used
- Who the information will/may be shared with (e.g. relevant professionals/agencies)
- Potential impact on the person(s) involved
- Whether the intended use is likely to lead to objections or complaints

Personal data and records will be maintained under appropriate conditions of security to prevent any unauthorised or accidental disclosure, in line with our Confidentiality Policy, and particular attention will be paid to the following aspects of storage and sharing:

- For physical records (paper/"hard copies"):
  - location of storage;
  - identification of those employees authorised to have access to specific data;
  - young persons/advocates authorised to have access to their personal records;
  - responsibilities for secure storage of the data at Orchard Therapeutic Care Ltd;
  - retention time (how long data records are kept for).
- For electronic/digital records:
  - responsibilities for implementing computer/digital security systems;
  - password-protection/encryption for access to sensitive data;
  - who is authorised to know passwords/encryptions;
  - how often passwords are changed;

- implications for networked systems;
- retention time;
- backup, control and management of personal data files;
- any special control requirements needed when online backup services are used.

- For non-text media (e.g. photos, video/audio recordings, biometric data):
  - responsibilities for implementing computer/digital security systems;
  - password-protection/encryption for access to sensitive data;
  - persons authorised to know passwords/encryptions;
  - how often passwords are changed;
  - retention time;
  - procedures for the control and management of personal data.

Where it is deemed necessary to divulge personal data to a third party, this will only be done with the express permission of the data subject. In this respect, both staff and young people and their families/advocates will also be advised that personal information held by Orchard Therapeutic Care Ltd may be shared with the regulating authority, as appropriate.

When personal data is being processed, administrative staff will take all reasonable precautions to prevent access to data by unauthorised persons:

- Records are locked away when not required, ensuring that digital records are password-protected and that passwords are regularly changed.
- Where practical, computer screens are tilted towards the user and away from the general office environment.
- Computers and devices are locked or switched off when unattended.

- Personal office housekeeping follows a "clear desk" policy, ensuring that confidential electronic files are encrypted when not in use and deleted unrecoverably when no longer needed, and that paper records are destroyed by cross-cut shredding.
- Confidential conversations are held in private and out of earshot of others.
- Information is transported/transferred securely, with end-to-end encryption for digital files.

Staff Responsibilities

This Policy does not form part of any employee's official contract of employment, but it is a condition of employment that staff will abide by the rules and Policies in effect at Orchard Therapeutic Care Ltd.

Employee information

All staff have a responsibility to:

- ensure that any personal details they provide to Orchard Therapeutic Care Ltd in connection with their employment are accurate and up to date
- inform Orchard Therapeutic Care Ltd of any changes to the information they have provided (e.g. address, bank details). Orchard Therapeutic Care Ltd cannot be held liable for any errors resulting from undeclared changes to staff information.

Data security

All staff are responsible for ensuring that:

- any personal data they collect, handle or hold is kept securely

- personal data is not disclosed orally, in writing or via the internet or any other means, deliberately or accidentally, to any unauthorised third party.

Staff should note that unauthorised data disclosures will usually be a disciplinary matter and may be considered gross misconduct in some cases. Staff should also be aware that they are expected to report to a relevant manager any action or inaction they witness or suspect within Orchard Therapeutic Care Ltd which constitutes a potential breach of data security or data protection laws (see Raising Concerns section).

Personal records should be kept in locked filing cabinets, drawers or safes. Digital records should be password protected and encrypted both on a local hard drive and a network drive and regularly backed up. Any removable storage media (e.g. USB drive, portable hard drive) must be kept in locked cabinets, drawers or safes.

Disaster Recovery

Orchard Therapeutic Care Ltd backs up all data every day and keeps multiple copies (at least one set for each day of the week and additional weekly sets, totaling at least one month's worth of data at any one time). Records of these backups and copies are kept.

Backup copies and software master copies are stored offsite. Any copies brought onsite are kept in fireproof and heatproof safes (fire-proofing alone is inadequate).

Backups are verified regularly by the software supplier.

Firewalls and anti-virus software are kept up-to-date and active on all computers within Orchard Therapeutic Care Ltd. Staff are trained in spotting and avoiding unsafe sites, viruses, malware, phishing scams. Service users and others who use computers onsite are also made aware of these threats and how to stay secure online.

Computers and other storage devices are protected from loss, theft or damage, and from electrical surges using protective plugs.

Orchard Therapeutic Care Ltd has plans in place for responding to network problems, power cuts, external data links and server failure. Paper forms of electronic data are used where necessary for temporary record-keeping.

Consent

The UK-GDPR sets a high standard for consent and requires positive opt-in for data collection. This means that consent is not presumed and individuals must explicitly agree to their data being collected, based on a clear explanation of how the information will be used and for what purpose. Pre-ticked boxes on forms or other methods of default consent are not allowed.

Consent means offering individuals real choice and control. This is especially important for young people who may be less confident about their rights with regard to their DATA. The principles of consent apply to everyone aged 16 or older whose personal information is processed by Orchard Therapeutic Care Ltd. This includes the young people using our service, the adults who work with them, their parents and other family members over 16. For children under 16, consent is obtained from their legal parent/guardian.

In line with our duties under the UK-GDPR, Orchard Therapeutic Care Ltd requests separate consent for separate information and will not use vague or blanket requests for consent. We specify what data we will collect, why and how it will be used. We keep records of consent and inform individuals of their right to withdraw consent at any time (and how to do this). No individual will be subject to any detriment for withholding or withdrawing consent.

However, it should be noted that consent is only one of several lawful bases for processing data. Orchard Therapeutic Care Ltd may process someone's data without explicit consent under any of the following conditions:

- Contract: if processing someone's personal data is necessary to fulfil Orchard Therapeutic Care Ltd.'s contractual obligations to that person (e.g. to provide a quote).

- Legal requirement: if processing personal data is necessary to comply with a common law or statutory obligation.
- Vital interests: if processing personal data is necessary to protect someone's life. (This is rare and cannot be relied on with regard to health data or other special category data if the individual can give consent.)
- Legitimate interests: if processing personal data is used in ways people would expect and have a minimal privacy impact, or where there is a compelling justification. (This is flexible and should be judged in context.)

Raising Concerns

The designated data controller, Ludivine Parmentier and the data protection officer, Jayne Andrews, are responsible for dealing with day-to-day matters concerning data protection. Any member of staff or other individual who considers that the Data Protection Policy has not been followed in respect of their own personal data should raise their concerns with one of the above-named persons.

Complying with the DPA and GDPR is crucial to fulfilling our duty of care as a registered provider of supported accommodation for young people. Therefore, Orchard Therapeutic Care Ltd urges any staff member who witnesses or suspects that a coworker is acting in breach of the Data Protection Policy or laws to notify a relevant manager as soon as possible, as outlined in our Whistleblowing procedures. Any staff member who makes a good-faith disclosure about possible misconduct will be protected from any reprisal or detriment for doing so. We will protect your confidentiality insofar as this aligns with our other obligations (e.g. safeguarding).

Data Protection Impact Assessment

Data Protection Impact Assessments (DPIAs) are recommended by the ICO as an essential part of accountability for organisations whose data processing is likely

to result in a high risk to the rights and freedoms of individuals. DPIAs help organisations to identify the most effective way to comply with their data protection obligations and meet individuals' expectations of informational privacy.

Key Question: What is Informational Privacy?

Informational privacy is the ability of a person to control, edit, manage and delete their personal information and to decide how and to what extent their information is communicated to others.

Actions that may violate an individual's informational privacy include collecting personal data in excess of what is needed, disclosing data without the subject's consent, misuse (using data for unofficial or undisclosed purposes), and collecting data through monitoring private communications (including message content and sender/recipient metadata).

As an organisation that processes sensitive personal data about young people, and where a data breach could jeopardise the health and safety of individuals, Orchard Therapeutic Care Ltd conducts a DPIA to identify and reduce the privacy risks of our service. The projected benefits of a DPIA include maximising the wellbeing and security of young people, demonstrating good practice to the ICO, improving transparency, and reducing the likelihood of privacy issues going forward.

In the context of DPIAs, "privacy risk" refers to a risk of harm resulting from violations of privacy. This primarily relates to informational privacy risk - the risk of harm through the improper processing of personal data. Informational privacy risks can arise if personal data held by the organisation is:

- inaccurate, insufficient or outdated
- excessive or irrelevant
- kept for longer than necessary

- disclosed to third parties without the subject's informed consent
- used in ways that are unspecified or unacceptable to the subject
- not kept securely
- not deleted securely.

The harm resulting from privacy risks may be clearly quantifiable (e.g. financial or job loss) or less defined (e.g. damage to social standing or relationships, or emotional harm). Sometimes harm might be less tangible or obvious to others, for example, the fear of identity theft from knowing that one's information security could be compromised. It can contribute to a reduced sense of personal autonomy or dignity, or anxiety about excessive surveillance.

Since the DPIA is intended to identify and reduce risks of harm, it can be considered a safeguarding measure. For more information on how we protect young people from harm, see our Safeguarding Policy.

The outcome of the DPIA should be a minimisation of privacy risks. As such, Orchard Therapeutic Care Ltd will develop an understanding of how it approaches the broad topics of privacy and privacy risks for its young people, staff and other potential data subjects. Understanding privacy risk in this context requires an understanding of the relationship between the organisation and the individual. Factors that may affect this include:

- Reasonable expectations of how the activity of individuals will be monitored
- Reasonable expectations of the level of interaction between an individual and an organisation
- Level of understanding of how and why particular decisions are made about people.

Orchard Therapeutic Care Ltd.'s DPIA process is followed in accordance with the ICO guidance. As part of the procedures, we:

- Describe the nature, scope, context and purposes of the data processing.

- Ask the persons processing our data to help us understand and document what they do and identify any associated risks.
- Consider how best to consult young people, their representatives and other relevant stakeholders.
- Ask for the advice of our data protection officer.
- Check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.
- Conduct an objective assessment of the likelihood and potential severity of any risks to individuals' rights and interests.
- Identify measures we can put in place to reduce high risks.
- Record our decisions in the outcome of the DPIA, including any difference of opinion with our data protection officer and consulted individuals.
- Implement the identified measures and integrate them into our business plan.
- Consult the ICO before processing data if we cannot mitigate high risk.
- Keep our DPIAs under review and revisit them when necessary.

Conducting and publicising a DPIA will help Orchard Therapeutic Care Ltd to build trust with the young people using the service. The actions taken during and after the DPIA process will improve our understanding of and relationships with our young people. There are also economic benefits to conducting a DPIA: identifying a problem early will generally require a simpler and less costly solution, and a DPIA can reduce ongoing costs by minimising the amount of information being processed where possible and devising more straightforward protocols for staff. Consistent use of DPIAs will increase the awareness of privacy and data protection issues within Orchard Therapeutic Care Ltd and ensure that data protection is a key consideration in all our activities.

Training

All staff at Orchard Therapeutic Care Ltd are trained in the principles and procedures of data protection and their legal obligations under the DPA and UK-GDPR as part of their induction and as applicable to their roles. Employees and managers are made aware of their responsibilities to consider and protect the privacy of young people, coworkers and others and keep all personal information secure. Staff will be informed of any changes to the relevant legislation or guidance and re-trained where necessary.

Policy Monitoring and Review

Compliance with this Policy and its procedures will be monitored by the Registered Manager, together with independent reviews by both internal and external audit on a periodic basis.

The Registered Manager is responsible for the monitoring, revision, and updating of this Policy.

This Policy will be kept under review in light of operational experience and national guidance. The first review will take place one year from adoption, and positive action will be taken to resolve any issues.

After reading this Policy, you should be able to:

- Understand what Data Protection is and why it is important;
- Understand how the Data Protection and GDPR Policy operates at Orchard Therapeutic Care Ltd and have an awareness of the actions we take in preventing, identifying and reporting concerns;
- Understand the role you play in the Data Protection and GDPR Policy.

If you have not understood any of these points, please ask your Line Manager or trainer for further help.

Authorisation and Signature

This Policy is the authorised version agreed by the CEO of Orchard Therapeutic Care Ltd.

All employees are expected to follow this Policy and failure to do so could result in disciplinary action.

Ludivine Parmentier

Chief Executive Officer