Larchfield House
Larchfield Road Maidenhead Berkshire SL6 2SJ

Review Sheet

Last Reviewed 24 May 2025

Last Amended 5 Jun 2024

This policy will be reviewed as needs require or at the following interval: Annual

Business Impact:	MEDIUM — Changes are important, but urgent implementation is not required, incorporate into your existing workflow.
Reason for this Review:	Scheduled review
Changes Made:	No
Summary:	This Overarching UK GDPR Policy and Procedure has been reviewed with no changes required at this time as guidance remains stable while the Data Protection and Digital Information Bill is progressed. The Further Reading section has been updated to reference additional relevant policies and procedures.
Relevant Legislation:	• HSCA 2008 (Regulated Activities) Regulations 2014 • UK GDPR (as defined in section 3(11) Data Protection Act 2018 • The Data Protection Act 2018
Underpinning Knowledge:	• Author: GOV UK, (2017), National Data Guardian – Review of Data security, consent and opt-outs [Online] Available from: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs [Accessed: 24/05/2025] • Author: Information Commissioner's Office, (2021), UK GDPR guidance and resources [Online] Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ [Accessed: 24/05/2025] • Author: Information Commissioner's Office (ICO), (2018), What are the conditions for processing? [Online] Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/#:~:text=Article%209%20%282%29%20%28a%29%20permits%20you%20to%20process,meet%20the%20usual%20UK%20GDPR%20standard%20for%20consent. [Accessed: 24/05/2025]
Suggested Action:	• Encourage sharing the policy through the use of the QCS App
Equality Impact Assessment:	QCS have undertaken an equality analysis during the review of this policy. This statement is a written record that demonstrates that we have shown due regard to the need to eliminate unlawful discrimination, advance equality of opportunity and foster good relations with respect to the characteristics protected by equality law.

Larchfield House
Larchfield Road Maidenhead Berkshire SL6 2SJ

1. Purpose

1.1 The purpose of this policy is to ensure that Larchfield House understands the key principles of UK GDPR.

1.2 This policy sets out the steps that need to be taken by Larchfield House to ensure that Larchfield House handles, uses and **processes personal data** in a way that meets the requirements of UK GDPR. It should be read alongside the suite of UK GDPR policies, procedures and guidance at Larchfield House.

1.3 This policy applies to all staff at Larchfield House who process personal data about other staff, Residentss and any other living individuals as part of their role.

1.4

Key Question	Quality Statements
WELL-LED	QSW5: Governance, management and sustainability
WELL-LED	QSW3: Freedom to speak up

1.5 Relevant Legislation

- HSCA 2008 (Regulated Activities) Regulations 2014
- UK GDPR (as defined in section 3(11) Data Protection Act 2018
- The Data Protection Act 2018

2. Scope

2.1 Roles Affected:

- All Staff

2.2 People Affected:

- Residentss

2.3 Stakeholders Affected:

- Family
- Advocates
- Representatives
- Commissioners
- External health professionals
- Local Authority
- NHS

3. Objectives

3.1 The objective of this policy is to ensure staff have a working knowledge into the principles and requirements of UK GDPR.

3.2 Alongside the suite of policies, procedures and guidance available, Larchfield House can demonstrate that appropriate steps are taken to ensure it complies with UK GDPR when handling and using personal data provided by both staff and Residentss.

3.3 This policy will assist with defining accountability and establishing ways of working in terms of the use, storage, retention and security of personal data.

3.4 This policy will assist with understanding the obligations of Larchfield House in respect of the rights of the staff and Residentss who have provided personal data and the steps Larchfield House should take if there is a personal data breach.

4. Policy

4.1 GDPR Background

GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998.

Following the UK's departure from the EU, UK GDPR was incorporated into domestic law that applies in the UK.

UK GDPR provides greater protection to individuals and places greater obligations on organisations than the pre GDPR data protection regime but can be dealt with in bite-size chunks. Compliance with data protection laws should enhance service provision and care provided by engendering trust between Larchfield House and Residentss.

4.2 All staff must ensure the ways in which they handle personal data meet the requirements of UK GDPR.

4.3 The Approach of Larchfield House to UK GDPR

Larchfield House is required to take a proportionate and appropriate approach to UK GDPR compliance. Larchfield House understands that not all organisations will need to take the same steps – it will depend on the volume and types of personal data processed by a particular organisation, as well as the processes already in place to protect personal data. Larchfield House understands that if significant volumes of personal data are processed, including **special categories of personal data**, or it has unusual or complicated processes in place in terms of the way personal data is handled, Larchfield House will consider obtaining legal advice specific to the processing conducted and the steps that may need to be taken.

4.4 UK GDPR and the Data Protection Act 2018 do not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.

4.5 Process for Promoting Compliance at Larchfield House

To ensure Larchfield House complies with UK GDPR and the Data Protection Act 2018, a suite of data protection policies and resources are available and should be read in conjunction with this overarching policy to provide a framework for compliance.

4.6 Overview of Key Terms, Key Principles and Documents

The key principles and themes of each of the documents listed above are summarised below:

Key Terms

UK GDPR places obligations on all organisations that process personal data about a data subject. A brief description of those three key terms is included in the Definitions section of this document and is expanded upon in the Key Terms Guidance.

The requirements that Larchfield House needs to meet vary depending on whether Larchfield House is a controller or a processor. In most cases, Larchfield House will be a controller. The meaning of 'controller' and 'processor', together with the roles they play under UK GDPR, are explained in the Key Terms Guidance. Larchfield House understands that it may be a controller in some circumstances and a processor in others.

Special categories of data attract a greater level of protection, and the consequences for breaching UK GDPR in relation to special categories of data may be more severe than breaches relating to other types of personal data. This information is also covered in more detail in the Key Terms Guidance.

Key Principles

There are 7 key principles of UK GDPR which Larchfield House must comply with. They are:

- Lawful, fair and transparent use of personal data
- Using personal data for the purpose for which it was collected
- Ensuring that the personal data is adequate and relevant
- Ensuring that the personal data is accurate
- Ensuring that the personal data is only retained for as long as it is needed
- Ensuring that the personal data is kept safe and secure
- Accountability - taking responsibility for what you do with personal data and how you comply with the other principles

Larchfield House must have appropriate measures and records in place to be able to demonstrate compliance.

These key principles are explained in more detail in the guidance entitled 'UK GDPR – Key Principles'.

Larchfield House recognises that, in addition to complying with the key principles, it must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. Larchfield House understands that a 'privacy by design' approach must be adopted. This means that data protection issues should be considered at the very start of a project, or engagement with a new Residents. Data protection should not be an after-thought. These ideas are also covered in more detail in the Key Principles Guidance.

Processing Personal Data

The provision of health or social care or treatment or the management of health or social care systems and services is expressly referred to in UK GDPR as a lawful basis upon which an organisation is entitled to process special categories of data.

In terms of other types of personal data, Larchfield House must only process personal data if it is able to rely on one of a number of grounds set out in UK GDPR. The grounds which are most commonly relied on are:

- The data subject has given their consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract with

the data subject; and

- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the data subject or another living person
- The processing is necessary to perform a task carried out in the public interest

The grounds set out above are explained in more detail in the guidance entitled 'UK GDPR – Processing Personal Data'.

Data Protection Officers

Larchfield House understands that some organisations will need to appoint a formal Data Protection Officer under UK GDPR (a '**DPO**'). The DPO benefits from enhanced employment rights and must meet certain criteria, so it is recognised that it is important to know whether Larchfield House requires a DPO. This requirement is outlined in the Appointing a Data Protection Officer Policy and Procedure.

Whether or not Larchfield House needs to appoint a formal Data Protection Officer, it will appoint a single person to have overall responsibility for the management of personal data and compliance with UK GDPR.

Data Security and Retention

Two of the key principles of UK GDPR are data retention and data security.

- Data retention refers to the period for which Larchfield House keeps the personal data that has been provided by a data subject. At a high level, Larchfield House must only keep personal data for as long as it needs the personal data
- Data security requires Larchfield House to put in place appropriate measures to keep data secure

These requirements are described in more detail in the Data Security and Data Retention Policy and Procedure.

Website Privacy and Cookies Policy and Procedure

Where Larchfield House collects personal data via a website, it understands that it will need a UK GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the purposes for which it is used and how long the personal data is kept. A template website policy is provided.

Wider Privacy Policies

Larchfield House understands that it is required to provide certain information to all individuals about whom it processes personal data, and that such information is usually provided via privacy policies. A template external and employee-facing privacy policy is provided.

The template privacy policy sits alongside a consent form which can be used to ensure that Larchfield House obtains appropriate consent, particularly from the Residents, to the various ways in which Larchfield House uses the personal data (where consent is the most appropriate ground for Larchfield House to rely upon). The consent form contains advice and additional steps to take if the Residents is a child or lacks capacity.

Subject Access Requests

One of the key rights of a data subject is to request access to, and copies of, the personal data held about them by an organisation. Where Larchfield House receives a subject access request, it understands that it will need to respond to it in accordance with the requirements of UK GDPR. To help staff at Larchfield House understand what a subject access request is and how they should deal with a subject access request, a Subject Access Requests Policy and Procedure is available to staff. A process map to follow when responding to a subject access request, as well as a subject access request letter template is also included.

The Rights of a Data Subject

In addition to the right to place a subject access request, data subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by Larchfield House. Not all rights apply in all circumstances. Rights of the data subject are covered in detail in the corresponding guidance.

Breach Notification Under UK GDPR

In certain circumstances, if there is a personal data breach (i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data), the ICO must be notified and potentially any affected data subjects. There are strict timescales in place for making such notifications. A policy and procedure for breach notification that can be circulated to all staff, together with a process map for Larchfield House to follow if a breach of UK GDPR takes place is available.

Larchfield House understands that this requirement is likely to have less impact on NHS organisations that are already used to reporting using the NHS reporting tool.

Transfer of Data

If Larchfield House wishes to transfer personal data to a third party, an agreement must be put in place to set out how the third party will use the personal data. If the third party is processing data on the instruction of Larchfield House, the contract must cover specific points set out in UK GDPR. Larchfield House must consider carrying out due diligence investigations on third party recipients of personal data of which Larchfield House is the controller.

Transfers of personal data outside of the UK and EEA may only be made under specific circumstances. This applies where a data processor processes personal data outside of the UK or EEA. Larchfield House understands that an adequacy decision has been made by the UK in respect of the EEA and by the EEA in respect of the UK, and that certain other countries are covered by adequacy decisions made by the UK and the EEA. Larchfield House understands that where an adequacy decision has been made, no further transfer safeguards need to be put in place. Larchfield House recognises that if no adequacy decision has been made in respect of the recipient country, transfer safeguards will need to be put in place and other aspects considered, including transfer impact assessments, before the transfer takes place. Guidance has been produced to explain the implications of transferring personal data in more detail. Larchfield House should consider seeking legal advice if it wishes to transfer personal data to a jurisdiction that does not benefit from a finding of adequacy.

Data Protection Impact Assessments

Larchfield House must carry out Data Protection Impact Assessments each time it processes personal data in a way that presents a 'high risk' for the data subject. Examples of when a Data Protection Impact Assessment should be conducted are provided in the relevant policy and procedure. Given the volume of special categories of data that are frequently processed by organisations in the health and care sector, there are likely to be a number of scenarios which require a Data Protection Impact Assessment to be completed.

4.7 Compliance with UK GDPR

Larchfield House understands that there are two primary reasons to ensure that compliance with UK GDPR is achieved:

- It promotes high standards of practice and care, and provides significant benefits for staff and, in particular, Residentss
- Compliance with UK GDPR is overseen in the UK by the ICO. Under UK GDPR, the ICO has the ability to issue a fine of up to £17.5 million or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences of non-compliance are therefore significant.

Larchfield House appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance and offers guidance to organisations about how to comply. A one-off, minor breach may not attract the attention of the ICO but if Larchfield House persistently breaches UK GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special category personal data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Larchfield House and its data protection policies and processes and to issue instructions for Larchfield House to comply or put right its data processing practices including requiring Larchfield House to stop providing services, or to notify data subjects of the breach, delete certain personal data held or prohibit certain types of processing.

5. Procedure

5.1 All staff must review the UK GDPR policies and procedures and guidance that are communicated to them.

5.2 Larchfield House will nominate a person to be the Data Protection Officer/Privacy Officer. This is currently Ulka Patel.

5.3 Larchfield House should ensure all staff understand the policies and procedures provided, including how to deal with a subject access request and what to do if a member of staff breaches UK GDPR.

5.4 Larchfield House will consider providing training internally about UK GDPR (in particular, the Key Principles of UK GDPR) to all staff members.

5.5 Larchfield House will delete any personal data that Larchfield House no longer needs, based on the results of the audit conducted, taking into account any relevant guidance, such as the Records Management Code of Practice - see link in the Further Reading section.

5.6 Larchfield House will, if necessary, put in place new measures or processes to ensure that personal data continues to be processed in line with UK GDPR.

5.7 Larchfield House will ensure it has privacy policies in place and will circulate them to data subjects as relevant.

5.8 Larchfield House will ensure that, where required, proper consent to the UK GDPR standard is obtained from each Residents. Larchfield House understands that the Consent

Form provided may be used for this purpose. Larchfield House will review the additional steps that it should take to ensure that it obtains consent from parents, guardians, carers or other representatives where Larchfield House works with children or those who lack capacity.

5.9 Larchfield House will ensure that processes and procedures are in place to respond to requests made by data subjects (including subject access requests) and to deal appropriately with any personal data breaches.

5.10 Larchfield House will maintain a log of decisions taken and incidents that occur in respect of the personal data processed by Larchfield House using the Data Protection Impact Assessment template at Larchfield House.

6. Definitions

6.1 Data Subject
- The individual to whom personal data relates

6.2 Data Protection Act 2018
- The Data Protection Act 2018 is a United Kingdom Act of Parliament

6.3 Personal Data
- Any information about a living person from which that person can be identified directly or indirectly including but not limited to names, email addresses, postal addresses, job roles, photographs, CCTV, online identifiers and special categories of data, defined below

6.4 Process or Processing
- Doing anything with personal data, including but not limited to collecting, storing, holding, using, amending, deleting or transferring it. You do not need to be doing anything actively with the personal data – at the point you collect it, you are processing it

6.5 Special Categories of Data
- Special categories of data include but are not limited to medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation, genetic and biometric data, trade union membership and political views

6.6 UK GDPR
- The UK GDPR is the retained EU law version of GDPR that forms part of English law

6.7 Information Commissioner's Office
- The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

6.8 Controller
- The main decision maker that exercises overall control over the purposes and means of processing personal data

6.9 Processor
- The entity acting on behalf of, and only in accordance with, the instructions of the controller

7. Key Facts - Professionals

Professionals providing this service should be aware of the following:

- This is the overarching policy and provides a high level reference to all areas that are important for compliance with UK GDPR
- Understanding of the content of this policy should be embedded with all staff at Larchfield House
- Larchfield House must appoint a person with overall responsibility for managing UK GDPR. This person may be an official Data Protection Officer (DPO) or a person appointed to oversee privacy, governance and data protection
- UK GPDR provides a high level of protection for staff and Residentss in respect of their personal data
- Larchfield House has adopted an appropriate and proportionate approach – what is right and necessary for Larchfield House may not be right for another organisation
- Achieving compliance with UK GDPR will not only reduce the risk of ICO enforcement or fines but will also promote a better quality service for Residentss and an improved working environment for staff
- Compliance is mandatory, not optional

8. Key Facts - People Affected by The Service

People affected by this service should be aware of the following:

- Your personal data will be protected and processed in accordance with the laws that apply to personal data
- There are various rights available to you in respect of your personal data
- There will be appropriate grounds in place for processing your information, which may be your consent
- In addition to the UK GDPR regulations, our staff will continue to follow confidentiality policies in relation to all aspect of your care

Further Reading

ICO - Information on countries benefiting from a finding of adequacy:

https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/international-data-transfers/#:~:text=Andorra%2C%20Argentina%2C%20Canada%20(commercial,a%20finding%20of%20adequacy%20about.

ICO - Appropriate Policy Document Template:

https://ico.org.uk/media/for-organisations/documents/2616286/appropriate-policy-document.docx

GOV.UK - New Health Data Security Standards and Consent/opt-out Model:

https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care

NHS England - Transformation Directorate - Records Management Code of Practice (provides guidance on how to keep records, including how long to keep different types of records.

https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

Other Policies and Resources

- Appointing a Data Protection Officer Policy and Procedure
- Data Security and Data Retention Policy and Procedure
- Website Privacy and Cookies Policy and Procedure
- Subject Access Requests Policy and Procedure
- Subject Access Requests Process Map
- Subject Access Requests - Request Letter
- Breach Notification Policy and Procedure
- Breach Notification Process Map
- External and Employee Privacy Policy and Procedure
- Data Quality Policy and Procedure
- Network Security Policy and Procedure
- National Data Opt-Out Policy and Procedure
- Clear Desk Policy and Procedure
- Consent Form
- Data Protection Impact Assessment (DPIA) Policy and Procedure
- Template Privacy Policy - External
- Template Privacy Policy - Employees

Outstanding Practice

To be "outstanding" in this policy area you could provide evidence that:

- The wide understanding of the policy is enabled by proactive use of the QCS App
- Larchfield House provides training to all staff in respect of UK GDPR and the new policies and processes that have been adopted
- Larchfield House conducts data protection impact assessments for each new processing activity carried out, whether or not the processing presents a 'high risk' to the data subjects
- There is evidence that Larchfield House conducts regular (6 monthly or annual) audits of the personal data that is processed to ensure continued compliance with UK GDPR
- Larchfield House can evidence that there are processes in place for ensuring it remains up to date with guidelines and recommendations relating to data protection,

including ICO guidance and guidance issued by NHS Digital and this information is effectively cascaded to all relevant staff