Nyton House – Data Protection with General Data Protection Regulation Policy

Aim and Scope of Policy

The policy, which aligns with UK data protection laws, demonstrates how this care service meets the data protection requirements outlined in the respective national care standards and regulations on good governance of record-keeping, resulting in records that are comprehensively fit for purpose and securely maintained.

The respective national care standards are as follows (refer to as required).

- England: Regulation 17: "Good Governance", of the Health and Social Care Act (Regulated Activities) Regulations 2014.
- Scotland: *My Support, My Life*, particularly Section 4: "I have confidence in the organisation providing my care and support".
- Wales: Regulation 59 "Records", of the Regulated Services (Service Providers and Responsible Individuals) (Wales) Regulations 2017.

All standards require complete, accurate, up-to-date records on service users, staff and other aspects concerning the running of the service to be kept in line with data protection, confidentiality, secure storage and authorised access policies and procedures.

This care provider also understands that all records required for the protection of service users and the effective and efficient operation of the care service should be collected, maintained, and kept in accordance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

This policy applies to all manual and electronic records kept by the service about service users, including those involved with them, whose personal data might be found on their records, all staff and any third parties (agencies and professionals) with whom anyone's personal data information held by the service might have to be disclosed or shared.

The policy should be used with other relevant record-keeping and information governance policies.

National Data Opt-Out policy

All regulated social care providers in England need to comply with the national data opt-out policy by 31 July 2022.

Introduced by the National Data Guardian in her *Review of Data Security, Consent and Opt-Outs* (2018), the national data opt-out provides everyone with the ability to stop health and adult social care organisations sharing confidential patient information for reasons other than direct care and treatment, such as research or planning.

Nyton House – Data Protection with General Data Protection Regulation Policy

National data opt-out applies where a service user is receiving social care provided, arranged or funded, in part or whole, by Local Authorities or the NHS in England. This does not affect individual care provision, where data processing is legally required, the service user has consented to processing or data has been appropriately anonymised.

It only applies when Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 ("Regulation 5 support") is utilised on a legal basis to process confidential patient information where processing would otherwise be a breach of confidentiality.

The term "confidential patient information" is a specific legal term which applies to information about a service user's health or social care that can identify them.

For more information, see National Data Opt-Out Policy in Data Protection and Privacy Notice for Service Users.

Compliance with data protection law and the GDPR during the coronavirus outbreak

The care service has noted and will comply with the advice and guidance of the Information Commissioner's Office during the current emergency. This is to the effect that the following apply.

1. Data protection law allows care providers to share information that is necessary to protect people from coronavirus and to provide the care required for their service users.

2. Information that is necessary for people's care can be shared legally and quickly, using, where appropriate, different forms of technology and applications. There will be no breach of data protection law if information is shared between services that help to achieve the sought-after wellbeing outcomes for service users.

3. The ICO is unlikely to act against any apparent breaches, eg of confidentiality, where it can be shown that the information disclosed or shared was for these purposes.

4. This includes information that can be used for public health purposes, although it will not usually require the disclosure of an individual service user's data.

5. Data protection law does not prevent a care service from disclosing information to third parties, such as family members, about how it and its service users are affected by the coronavirus outbreak, eg if it has service users with the virus or their relative has tested positive for the virus.

6. Wherever possible, such information will not reveal identities unless there are good reasons for doing so, for example, to prevent a person from coming into contact with an infected person or because of their concerns for a person's welfare as a family member.

7. In these instances, the service will follow a "need to know" principle. It will make all reasonable efforts to obtain people's consent to the disclosure of any coronavirus-related information, though this might not be possible in every situation and sometimes it will be necessary to exercise discretion.

8. Data submitted to the Capacity Tracker as outlined in DHSC *Admission and Care of Residents in a Care Home During COVID-19*is not within the scope of the national data opt-out policy.

In line with ICO guidance, these elements of the policy will be reviewed once the emergency period is over.

Policy Statement

Nyton House Limited recognises it must keep all records required for the protection and wellbeing of service users, and those for the effective and efficient running of the care service such as staff records to comply currently with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), which came into force in May 2018.

In line with its registration under the Data Protection Act, and to comply with GDPR, the service understands that it will be accountable for the processing, management and regulation, storage and retention of all personal data held in the form of manual records and on computers.

This means that all personal data obtained and held by the care service to carry out its activities as a registered care provider must:

- have been obtained reasonably and lawfully
- held for specified and lawful purposes as an organisation that is carrying out a public duty
- processed in recognition of persons' data protection rights, which are described in GDPR in terms of the right:
  - to be informed
  - to have access
  - for the information to be accurate and for any inaccuracies to be corrected
  - to have information deleted (eg if inaccurate or inappropriately included)
  - to restrict the processing of the data to keep it fit for its purpose only
  - to have the information sent elsewhere as requested or consented to (eg in any transfer situation)
  - to object to the inclusion of any information (eg if considered to be irrelevant)

  - to regulate any automated decision-making and profiling of one's personal data

- be adequate, relevant and not excessive in relation to the purpose for which it is being used
- be kept accurate and up to date, using whatever recording means are used or agreed (eg manual or electronic)
- not be kept for longer than is necessary for its given purpose (eg in line with agreed retention protocols for each type of record)
- have appropriate safeguards against unauthorised use, loss or damage with clear procedures for investigating any breaches of the data security
- comply with the relevant GDPR procedures for international transferring of personal data.

In line with the Data Protection Act 2018 and the GDPR, the care service has a data controller and a nominated data protection officer, who is responsible for the safekeeping and safeguarding of all personal data held by the care service.

Procedures

The service has taken the following steps to protect everyone's personal data, which it holds or to which it has access so that it complies with current data protection laws and GDPR.

1. It appoints or employs staff with specific responsibilities for:

    a. the processing and controlling of data (data controller)

    b. the comprehensive reviewing and auditing of its data protection systems and procedures (data protection manager or auditor)

    c. overviewing the effectiveness and integrity of all the data that must be protected (data protection officer).

    There are clear lines of responsibility and accountability for these different roles.

    Note: The organisation of these roles and data protection functions will vary, but it is essential to specify who is responsible for what.

2. It provides information to its service users and others involved in their care on their data protection rights, national data opt-out policy, how it uses their personal data, and how it protects it. The information includes the actions service users and staff can take if they think that their data has been compromised in any way (eg through the complaints procedure or grievance procedure in the case of staff).

3. It provides its staff with information and training to make them aware of the importance of protecting people's personal data, to teach them how to do this, and to understand how to treat information confidentially.

4. It can account for all personal data it holds, where it comes from, and who it is and might be shared with.

5. It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the service.

6. It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions.

7. It has policies and procedures for enabling service users and/or staff to have access to their personal information, and for the making of subject access requests that are in line with GDPR.

8. It has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences (eg fine).

9. [Where applicable.] If the organisation holds personal data on any child under the age of 16, it informs the child how their data is being protected in ways that the child can understand, and has procedures in place to obtain consent of the responsible parent for obtaining and using the child's data.

Training

New staff must read and understand the policies on data protection and confidentiality as part of their induction.

All staff receive training covering basic information about confidentiality, data protection and access to records.

Training in the correct method for entering information in service users' records is given to all care staff.

The nominated data controller/auditors/protection officers for the care service are trained appropriately in their roles under GDPR.

Nyton House – Data Protection with General Data Protection Regulation Policy

All staff who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the organisation of any potential lapses and breaches of the service's policies and procedures.

Guidance for Data Transparency, Consent and Right of Access

Data Controller – Harvey Hillary

Data Processor – Sally Lewis

Data Transparency

- Staff given notice of all information held, length of time held for and purpose for holding data
- Data Policy on Website: Download from homepage

Consent

- Staff - GPPR Consent requested for holding Personal and Sensitive Data for use in relation to Internal HR – Signed by all staff
- Service users - GDPR Consent requested for holding Personal and Sensitive Data for use in relation to the provision of care
- Consent will be requested annual via e-signature or signed in person. The signature of the LPOA will be required where a service user does not have capacity

Access to Personal Information

- Information can be provided to the data subject in writing, electronically or verbally. GDPR information must be supplied by Nyton House Limited without undue delay, but at latest within one month

Nyton House – Data Protection with General Data Protection Regulation Policy

Your Data – Staff

Personal Data	Retention	Checked for Accuracy
DOB	6mths after leaving	yearly
National Insurance Number	6mths after leaving	
Contact: Address, Previous addresses (last 5yrs) Email Address, Mobile, Home Phone	6mths after leaving	Yearly
Marital Status	6mths after leaving	Yearly
Driving Licence	6mths after leaving	Yearly
Passport Number	6mths after leaving	Yearly
Emergency Contract	6 months after leaving	Bi-yearly
Sensitive Data		
Health Assessment – Night Worker	6months after leaving	Yearly
Kitchen Staff Health Assessment	6 months after leaving	Yearly
Employment Questionnaire (Health)	6months after leaving	Na
Fit for work assessment or GP Notes relating to Health	6months after leaving	Consent requested
Sickness, Injury and Absence Records including condition, medical reports etc	6months after leaving or 2yrs after audit whichever is sooner	Yearly
DBS Certificate Information	6months after leaving	All Staff every 3yrs
Driving offences	While employed	Yearly
Employment Data		
Recruitment – CV, References	6yrs after leaving – unsuccessful candidates retained for 6months	
Personnel Files – including Training, working time records, Pay and Benefits records including pension	6 years after leaving	Yearly
Disciplinary Records	6yrs after leaving	Yearly
Accident Log	3 years from the date of last entry	Yearly
Annual Leave records	2 years after	Yearly
ESR Staff records – Diversity data	Retaining permanently (anonymous)	Yearly

Nyton House – Data Protection with General Data Protection Regulation Policy

Your Data – Service User

Personal Data	Time	Checked for Accuracy
DOB	While resident	
Next of Kin	While resident	Yearly
Address	While resident	
Primary nurse	While resident	
GP name	While resident	Yearly
Social worker name	While resident	Yearly
Image	While resident	Yearly
Biographical info	While resident	
Image – Facebook and website	While resident	Consent Requested yearly
Sensitive Data		
Life choices and preferences	While resident	
Regions beliefs	While resident	
Care Assessment	While resident	
Falls Record		
Medication History		
Decision Making Capacity		
Bank Details (where financial capacity exists)		

Transparency - Data Policy on Website

Consent - GDPR Consent requested for holding Personal and Sensitive Data for use in relation to the provision of care, contractual

Your Data – Service User

Personal Data	Time	Checked for Accuracy
Contact details: Inc. email, address, telephone	When under contract + 2 years	Yearly
Lasting Power of attorney	While under contract	When LPA is in place
Payee Bank Details	When under contract	Yearly

Transparency - Data Policy on Website

Consent - GDPR Consent requested for holding Personal and Sensitive Data for use about the provision of care, contractual

Nyton House – Data Protection with General Data Protection Regulation Policy

Signed 

Date: 17/06/2025

Policy review date: June 2026
