

General Data Protection Regulation Policy (GDPR)

Reader Information	
Policy Title	General Data Protection Regulation Policy (GDPR)
Policy Number (Corporate/Clinical)	0001
Primary Author Contact Details	Kevin Foley
Original Publication Date	April 2019
Last Reviewed Date	January 2023
Next Review Date Due	January 2025
Policy Description	
Ratified	
Cross Reference	Retention of Records Policy, Disclosure and Barring Service Policy 2016, Confidentiality Policy, Records Management Policy, Records Retention Policy, Rectification and Erasure procedure, Subject Access Request Policy and Procedure, Audit Policy, Incident Response Policy and Procedure, ICT acceptable Use Policy, Audit Policy
Superseded Documents	

1. **Introduction**

Julia's House(JH) needs to collect and use certain types of information about the people it comes into contact with such as Employees, Volunteers, Patients and their families, Supporters and Donors in order to carry on our work. This personal information must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under 2018 EU General Data Protection Regulation GDPR).

2. **Purpose**

The Interpretation of GDPR is supported by this policy and Julia's House (JH) procedures, policies and guidance (The Information Governance Framework IGF). They are designed to ensure that JH is compliant with the law. Guidance is given to minimise any risk and therefore protect the individuals as well as balancing this with the ability to continue to deliver the various functions of JH.

3. **Policy**

This policy applies to all JH staff and volunteers.

4. Data Controller

The person or team who determines the purpose for which and the manner in which any personal data at JH will be held or used. They are also responsible for notifying the Information Commissioners Office (ICO) of the data it holds, or is likely to hold and the general purposes that the data will be used for. This is reviewed annually as part of the registration process with the ICO.

5. Disclosure

- 5.1 JH may share data with third parties who are working on behalf of JH, and have signed confidentiality agreements. In no circumstances would JH sell an individual's personal data.
Individuals will be made aware in most circumstances by notices located on the website, on application forms and other relevant documentation.
- 5.2 There are circumstances where the law allows JH to disclose data (including sensitive data) without the individual's consent. These are:
 - 5.2.1 Carrying out a legal duty or as authorised by the Secretary of State
 - 5.2.2 Protecting vital interests of an individual or other person
 - 5.2.3 The individual has already made the information public
 - 5.2.4 Conducting any legal proceedings, obtaining legal advice or defending any legal rights
 - 5.2.5 Monitoring for equal opportunities purposes – i.e. race, disability or religion however always anonymised
 - 5.2.6 Providing a confidential service where the individual's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill individuals to provide consent signatures.
- 5.3 There are data protections principles set out as the main responsibilities for organisations which means data must be:
 - 5.3.1 Processed lawfully, fairly and in a transparent manner in relation to individuals;
 - 5.3.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
 - 5.3.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 5.3.4 Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- 5.3.5 Kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for long periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisation measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- 5.3.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

6. Data Collection

- 6.1 JH will ensure that data is collected within the boundaries defined within this policy. This applies to data that is collected in person (face to face or over the telephone), electronically or by completing a form. It applies to any location that is being used by staff, volunteers or contractors to deliver JH related business.
- 6.2 When collecting data, JH will ensure, wherever possible, that there is a fair processing notice in place and that the individual:
 - 6.2.1 Clearly understands why the information is needed, what it will be used for and what the consequences are.
 - 6.2.2 Understands who the data may be shared with and why.
 - 6.2.3 Has the option to agree to share the data.
 - 6.2.4 Grants explicit written or verbal consent to collect and share sensitive data (health related information) wherever possible.
 - 6.2.5 Gives explicit consent to contact via email.
 - 6.2.6 Is competent to give consent and has given so freely without any duress.
- 6.3 The above points indicate that the individual will have enough information for them to give informed consent. Any concerns regarding competence should be referred to a health care professional.

7. Data Storage

Information and records relating to individuals will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately in line with the Records Retention policy.

It is JH responsibility to ensure all personal and company data is non recoverable from any computer system previously used within the organisation which has been passed on to a third party.

8. Data Access

- 8.1 All individuals have the right to access the information JH holds about them. JH will also take reasonable steps to ensure that this information is kept up to date.
- 8.2 All employees have the responsibility of ensuring information stored about an individual is factual and not subjective.
- 8.3 JH ensures that:
 - 8.3.1 Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
 - 8.3.2 Everyone processing personal information is appropriately trained to do so.
 - 8.3.3 Everyone processing personal information is appropriately supervised.
 - 8.3.4 Everyone processing personal information will report a suspected or actual breach of data management using the Incident Response reporting procedure.
 - 8.3.5 Anybody wanting to make enquiries about handling personal information knows what to do.
 - 8.3.6 It deals promptly and courteously with any enquiries about handling personal information.
 - 8.3.7 It describes clearly how it handles personal information.
 - 8.3.8 It will regularly review and audit the ways it holds, manages and uses personal information.
 - 8.3.9 It regularly assesses and evaluates its methods and performance in relation to handling personal information.
 - 8.3.10 All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.
 - 8.3.11 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments in the law.

9. Consent

- 9.1 Under GDPR, a lawful basis needs to be identified before personal data can be processed. If there is personal data identified, then consent must be sought.
- 9.2 To be considered a lawful basis to process data one of the following must apply:
 - 9.2.1 Processing is necessary for the performance of a contract with the individual, or to take steps to enter a contract. This could be to fulfil an employment contract, or a contract to provide goods or services.
 - 9.2.2 Processing is necessary to comply with a legal obligation.
 - 9.2.3 Processing is necessary to protect the vital interests of an individual or another person.

- 9.2.4 Processing is necessary to fulfil a task that is in the public interest or in the exercise of official authority vested in the Data Controller.
- 9.2.5 Processing is necessary for the purposes of legitimate interests of the organisation and those legitimate interests are not outweighed by possible harm to the individual's rights and interests.
- 9.3 Consent must be:
 - 9.3.1 Freely given: the individual has choice and control on how their personal data may be used.
 - 9.3.2 Specific and informed: the individual understands all the purposes for which their data may be used. If there are multiple purposes, consent must be sought for each.
 - 9.3.3 Unambiguous: the individual knows what they have consented to, and that they have given their consent.
 - 9.3.4 A deliberate action by the individual e.g. signing / verbal / electronic binary choice options.
 - 9.3.5 Consent may be implied, for example when completing a survey. The personal data provided may be used for the purposes stated in the survey. The data may not be used for any other purpose unless specific consent has been asked and an action has been taken to indicate it has been given.
- 9.4 When consent is not required:
 - 9.4.1 Explicit consent is not required for the processing of special categories of personal data when processing is necessary for the provision of health care, treatment or social care.
For Julia's House this applies across the range of services that we offer to our patients and their families.
 - 9.4.2 A similar exemption applies to the processing of personal data if the processing is necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social services.

10. Childs Data Protection Rights

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

- 10.1 Children have the same rights as adults over their personal data. these include the rights to access their personal data; request rectification; object to processing and erasure.
- 10.1.2 JH must ensure that a child can exercise their data protection rights easily and in such a way that the child can understand.
- 10.1.3 JH allow competent children to exercise their own data protection rights.

10.1.4 If the original processing was based on consent provided when the individual was a child, then JH will comply with a request for erasure where possible.

References

Information Commissioners Office - <https://ico.org.uk/for-organisations/>

EU General Data Protection Regulation (GDPR) – May 2018

Data Protection Act 1998