


Data Protection Policy and Procedure Manual

Your Voice in Health & Social Care (YVHSC)

45 St Mary's Road, Ealing W5 5RG | 020 3603 2438 | www.yvhsc.org.uk

Revision No	Date	Signature
Issue Date	24/08/2021	
Next Review Date	August 2024	

DATA PROTECTION POLICY

CONTENTS

1	PURPOSE	3
2	SCOPE	3
3	POLICY STATEMENT	3
	3.1. Governance	3
	3.2. Data Protection Principles.....	4
	3.3. Data collection	5
	3.4. Data Use	6
	3.5. Data Retention	7
	3.6. Data Protection	8
	3.7. Data subject Requests.....	9
	3.8. Law Enforcement Requests & Disclosures.....	9
	3.9. Data Protection Training	9
	3.10. Data Transfers	9
	Data Transfers between YVHSC services/entities	10
	Data Transfers to Third Parties	10
	3.11. Complaints handling	11
	3.12. Breach Reporting.....	11
	Breach Notification procedure.....	11
4	Data Protection impact Assessment.....	11
	When is DPIA necessary	11
	DPIA PROCEDURE	12
5	Data Security	12
6	Roles and Responsibilities	13
6.1	Implementation	13
	6.2 Support, Advice and Communication	13
7	REVIEW	13
8	RECORDS MANAGEMENT	13
9	TERMS AND DEFINITIONS.....	13
10	APPROVAL AND REVIEW DETAILS	14

1 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the GDPR.

2 SCOPE

This policy applies to all Your Voice in Health & Social Care (YVHSC) employees and all third parties responsible for the processing of personal data on behalf of all YVHSC services/entities.

3 POLICY STATEMENT

YVHSC is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of YVHSC employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a YVHSC contact (i.e. the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. YVHSC, as a Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose YVHSC to complaints, regulatory action, fines and/or reputational damage.

YVHSC's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all YVHSC employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1. Governance

3.1.1. Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, YVHSC has appointed a Data Protection Officer. The Data Protection Officer operates with independence and is supported by suitably skilled individuals granted all necessary authority. The Data Protection Officer reports to YVHSC's CEO. The Data Protection Officer's duties include:

- Informing and advising YVSHC and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of YVHSC's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of YVHSC's current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing senior managers, officers, and directors of YVHSC of any potential corporate, civil and criminal penalties which may be levied against YVHSC and/or its employees for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to a YVHSC service/entity
- receives personal data from a YVHSC service/entity
- has access to personal data collected or processed by YVHSC

3.1.2. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all YVHSC services/entities in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
 - ✓ Raising awareness.
 - ✓ Training of employees.
- The effectiveness of data protection related operational practices, including:
 - ✓ Data subject rights.
 - ✓ Personal data transfers.
 - ✓ Personal data incident management.
 - ✓ Personal data complaints handling.
 - ✓ The level of understanding of data protection policies and privacy notices.
 - ✓ The currency of data protection policies and privacy notices.
 - ✓ The accuracy of personal data being stored.
 - ✓ The conformity of data processor activities.
 - ✓ The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Officer, in cooperation with key business stakeholders from each YVHSC service/entity, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the YVHSC management team.

3.2. Data Protection Principles

YVHSC has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, YVHSC must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means YVHSC must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means YVHSC must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means YVHSC must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means YVHSC must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be 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. YVHSC must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for, and be able to demonstrate compliance. This means YVHSC must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. Data collection

3.3.1. Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

3.3.2. Data subject consent

Each YVHSC service/entity will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, YVHSC is committed to seeking such consent. The Data Protection Officer, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data.

3.3.3. Data subject Notification

Each YVHSC service/entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. When the data subject is asked to give consent to the processing of personal data and

when any personal data is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.4. Data Use

3.4.1. Data processing

YVHSC uses the personal data of its contacts for the following broad purposes:

- The general running and business administration of YVHSC services/entities.
- To provide services to YVHSC's stakeholders.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by YVHSC to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that YVHSC would then provide their details to third parties for marketing purposes.

Each YVHSC run service will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, YVHSC will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

- In any circumstance where consent has not been gained for the specific processing in question, YVSHC will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.

3.4.2.Children's Data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

3.4.3.Data Quality

Each YVHSC run service will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by YVHSC to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, in so far as:
 - ✓ a law prohibits erasure.
 - ✓ erasure would impair legitimate interests of the data subject.
 - ✓ the data subject disputes that their personal data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

3.4.4.Digital Marketing

As a general rule YVHSC will not send promotional or direct marketing material to a YVHSC Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any YVHSC service/entity wishing to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Protection Officer. Where personal data processing is approved for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5. Data Retention

To ensure fair processing, personal data will not be retained by YVHSC for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which YVHSC services/entities need to retain personal data is set out in YVHSC '*Data Retention Policy*'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Retention Requirements

YVHSC has set the following guidelines for retaining all personal data as defined in the data privacy policy.

- Website visitor data will be retained as long as necessary to provide the service requested/initiated through the YVHSC website.

- Contributor data will be retained for the year in which the individual has contributed and then for 2 years after the date of the last contribution. Financial information will not be retained longer than is necessary to process a single transaction.
- Event participant data will be retained for the period of the event, including any follow up activities, such as the distribution of reports, plus a period of 2 years.
- Program participant data (including sign in sheets) will be retained for the duration of the grant agreement that financed the program plus any additional time required under the terms of the grant agreement.
- Personal data of subgrantees, subcontractors and vendors will be kept for the duration of the contract or agreement.
- Employee data will be held for the duration of employment and then 1 month after the last day of employment.
- Data associated with employee wages, leave and pension shall be held for the period of employment, with the exception of pension eligibility and retirement beneficiary data which shall be kept for 1 year..
- Recruitment data, including interview notes of unsuccessful applicants, will be held for 1 month after the closing of the position recruitment process.
- Consultant (both paid and pro bono) data will be held for the duration of the consulting contract plus 1 month after the end of the consultancy.
- Board member data will be held for the duration of service on the Board plus for 1 month after the end of the member's term.
- Data associated with tax payments (including payroll, corporate and VAT) will be held for 1 year.
- Operational data related to program proposals, reporting and program management will be held for the period required YVHSC, but not more than 2 years.

Data Destruction

Data destruction ensures that YVHSC manages the data it controls and processes it in an efficient and responsible manner. When the retention period for the data as outlined above expires, YVHSC will actively destroy the data covered by this policy. If an individual believes that there exists a legitimate business reason why certain data should not be destroyed at the end of a retention period, he or she should identify this data to his/her supervisor and provide information as to why the data should not be destroyed. Any exceptions to this data retention policy must be approved by YVHSC's CEO in consultation with the company's DPO. In rare circumstances, a litigation hold may be issued by legal counsel prohibiting the destruction of certain documents. A litigation hold remains in effect until released by legal counsel and prohibits the destruction of data subject to the hold.

3.6. Data Protection

Each YVHSC service/entity will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.

- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

3.7. Data subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure. If an individual makes a request relating to any of the rights listed above

YVHSC will consider each such request in accordance with all applicable data protection laws and regulations based upon a request made in writing/email to: dpo@yvhsc.org.uk

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights..

3.8. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If an YVHSC service/entity processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any YVHSC service/entity receives a request from a court or any regulatory or law enforcement authority for information relating to an YVHSC contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

3.9. Data Protection Training

All YVHSC employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each YVHSC run service will provide regular Data Protection training and procedural guidance for their staff.

3.10. Data Transfers

YVHSC services/entities may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. YVHSC services/entities may only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject

- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

Personal data is considered confidential. Any unauthorised processing of these data by employees/contractors is strictly forbidden. Employees/contractors will only have access to personal data as appropriate for the type and purpose of the service task in question. This requires the implementation of roles and responsibilities.

Employees/contractors are forbidden to use Personal Data for private or commercial purposes, disclose them to unauthorised persons, or make them available in any other way including YVHSC servers or email.

YVHSC has to inform employees/contractors at the beginning of the work relationship about the obligation to protect the confidentiality of personal data and information. This obligation remains in effect even after the end of the employment/contractual period.

Data Transfers between YVHSC services/entities

- 3.1 In order for YVHSC to carry out its operations effectively across its various services/entities, there may be occasions when it is necessary to transfer personal data internally from one Entity to another, or to allow access to the personal data from an overseas location. Should this occur, the YVHSC service/entity sending the personal data remains responsible for ensuring protection for that personal data.
- 3.2 YVHSC handles the transfer of personal data between YVHSC run services, where the location of the recipient entity is a third country, using the binding corporate rules transfer mechanism. Binding corporate rules provide legally binding, enforceable rights on data subjects with regard to the processing of their personal data and must be enforced by each approved YVHSC service/entity, including their employees. Only transfer the minimum amount of personal data necessary for the particular purpose of the transfer (for example, to fulfil a transaction or carry out a particular service). Ensure adequate security measures are used to protect the personal data during the transfer (including password-protection and encryption, where necessary).

Data Transfers to Third Parties

- 3.3 Each YVHSC service/entity will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, each YVHSC service/entity will first identify if, under applicable law, the third party is considered a data controller, or a data processor of the personal data being transferred.
- 3.4 Where the third party is deemed to be a data controller, the YVHSC service/entity will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the controller to clarify each party's responsibilities in respect to the personal data transferred. Where the third party is deemed to be a data processor, the YVHSC service/entity will enter into, in cooperation with the Data Protection Officer, an adequate processing agreement with the data processor. The agreement must require the data processor to protect the personal data from further disclosure and to only process personal data in compliance with YVHSC's instructions. In addition, the agreement will require the data processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches.

3.11. Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer at dpo@yvhsc.org.uk. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.12. Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail, by calling YVHSC's head office. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, YVHSC Management Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

Breach Notification procedure

- All personal data breaches must be reported immediately to YVHSC's Data Protection Officer.
- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Data Protection Regulator is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 3.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of YVHSC's Data Protection Officer;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by YVHSC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

4 Data Protection impact Assessment

Data Protection Impact Assessments (DPIA) are used to identify and mitigate against any data protection related risks arising from a new project, service, product, or process, which may affect the organisation (Data Controller) or the individuals (Data Subjects).

When is DPIA necessary

4.1 DPIA is necessary:

- Before the implementation of new services or processes, or before the modification of existing services or processes;

- Data processing is likely to result in a high risk to the rights and freedoms of individuals.

4.2 Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- Large scale, systematic monitoring of public areas (CCTV).

DPIA PROCEDURE

Steps for conducting DPIA

- 4.3 **Describe data flows.** Identify how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. Identify what kinds of data will be used as part of the new (or modified) system or process and who will have access to the data. Populate Section 1 of the Data Protection Impact Assessment (DPIA) Form.
- 4.4 **Identify data protection and related risks.** Identify all risks to Data Subjects or to the organisation (Data Controller) that are related to personal data protection. For each risk assign a risk category (High/Medium/Low) and populate the appropriate columns in Section 2 of the Data Protection Impact Assessment (DPIA) Form.
- 4.5 **Assign risk mitigation measures.** For each risk assign risk mitigation measures. Focus on mitigating measures for risks with High and Medium impact category. Populate the last column in Section 2 of the Data Protection Impact Assessment (DPIA) Form.
- 4.6 **Further actions.** Consider if the Regulator should be consulted for the DPIA. Plan regular DPIA reviews and updates.

5 Data Security

YVHSC takes the protection and security of its customers' data very seriously. YVHSC manages the security of its customers' data.

Our services collect limited information about customers - name, email address and phone - which are retained for account creation. Postal address is requested and retained by YVHSC.

YVHSC takes the integrity and protection of customers' data very seriously. We maintain history of two kinds of data: application logs from the system, and customers' data. All data is stored in the Informatics system.

Our IT team ensures that different environments are in use for development and testing purposes, access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification, with Segregation of Duties built in, and reviewed on a quarterly basis.

Operational Security

YVHSC understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. The company has clear change management processes, logging and monitoring procedures, and fall back mechanisms which have been set up as part of its operational security directives.

All employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security- related policies.

Confidential information about the company is available for access only to select authorised YVHSC employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organisational security policies. Security incidents (breaches and potential vulnerabilities) can be reported by patients through our local service websites or directly at yvpsc.org.uk or via email: dpo@yvpsc.org.uk.

The company's *Data Protection Policy* is approved by the Board of Directors.

Network Security

The YVHSC office network where updates are developed, deployed, monitored and managed is secured by industry-grade firewalls and antivirus software, to protect internal information systems from intrusion and to provide active alerts in the event of a threat or an incident. Firewall logs are stored and reviewed periodically. Access to the production environment and remote access is possible only via the office network. Audit logs are generated for each remote user session and reviewed. Also, the access to production systems are always through a multi-factor authentication mechanism.

All YVHSC products are hosted in Cloud Services, with security managed by IT Trouble Free and White Bear Group. Their team monitors the infrastructure 24x7 for stability, intrusions and spam using a dedicated alert system. Every three months, end-to-end vulnerability assessments and penetration tests are performed. The Informatics application has an in-built spam protection system for businesses that use it, while our IT team monitors and blocks individual accounts and IP addresses which attempt to access the YVHSC applications.

6 Roles and Responsibilities

6.1 Implementation

The management team of each YVHSC service/entity must ensure that all YVHSC employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, each YVHSC service/entity will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by YVHSC.

6.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer on +44 (0) 0203 886 0839 or email dpo@yvpsc.org.uk.

7 REVIEW

This policy will be reviewed every year, unless there are any changes to regulations or legislation that would enable a review earlier.

8 RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised YVHSC recordkeeping system. All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

9 TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the

European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

10 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Tim Spilsbury – CEO YHSC
Data Protection Officer	Ian Hughes
Next Review Date	01/08/2024