Title	Data Protection Policy
Process Owner	Management
Date Created	22/02/2021
Publish Date	04/03/2021
Approved By	CEO
Summary	Policy detailing the requirements for the organisation with regards to the Data Protection Act.
Classification	Public
Standard	All
Version	1.0

Change Record
Enter any changes to the document within the tag below…
Reviewed and ready for internal audit
Overwrite the content of the tag, this will create each change you have made to the document and record it in ISOportal

Data Protection Policy

V-Health Passport holds and processes information about employees, and other data subjects for administrative and commercial purposes. When handling such information, V-Health Passport, and all staff or others who process or use any personal information, must comply with the Data Protection Principles.

In summary, these state that personal data shall:

- be processed fairly and lawfully,
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose,
- be adequate, relevant and not excessive for the purpose
- be accurate and up-to-date,
- not be kept for longer than necessary for the purpose,
- be processed in accordance with the data subject's rights,
- be kept safe from unauthorised processing, and accidental loss, damage or destruction,
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.

In relation to customer data, V-Health Passport are considered data processors and therefore the liability is the responsibility of the customer.

In relation to internal data V-Health Passport are the data controllers and have implemented policies and security protections

Applicable Legislation

- Data Protection Act
- General Data Protection Regulations

Authorities / Responsibility

V-Health Passport are registered with the ICO.
Registration number: ZA785511
Expiry date: 04/09/2021

V-Health Passport have designated a Data Protection Officer (DPO): Louis-James Davis - CEO

Definitions

- "Data controller" who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
- "Other data subjects" and "third parties" may include contractors, suppliers, contacts, referees, friends or family members.

- "Processing" refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

Notification of Data Held

V-Health Passport shall notify all staff and other relevant data subjects of the types of data held and processed by V-Health Passport concerning them, and the reasons for which it is processed. The information which is currently held by V-Health Passport. This is detailed within our Privacy Statement; this is available on our website.

Data Protection Information

Information provided by staff to V-Health Passport

All staff shall:

- ensure that all personal information which they provide to V-Health Passport in connection with their employment is accurate and up to date;
- inform V-Health Passport of any changes to information, for example, changes of address;
- check the information which V-Health Passport shall make available from time to time, in written or automated form, and inform V-Health Passport of any errors or, where appropriate, follow procedures for up-dating entries on computer forms.
- V-Health Passport shall not be held responsible for errors of which it has not been informed.

Information held or processed by staff

Staff shall ensure that:

- all personal information is kept securely;
- personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. Unauthorised disclosure may be a disciplinary matter and may be considered gross misconduct in some cases.

Rights to Access Information

- Personnel and other data subjects in V-Health Passport have the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the appropriate designated data controller.
- V-Health Passport aims to comply with requests for access to personal information as quickly as possible; but will ensure that it is provided within 30 days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing by the designated data controller to the data subject making the request.

- Data requests will be evaluated on an individual basis. The number of data requests in a given time period will be assessed. Multiple data requests over 6 months time period will result in charges being made for the data request, if this is an external data subject.

Subject Consent

- In some cases, such as the handling of sensitive information or the processing of research data, V-Health Passport is entitled to process personal data only with the consent of the individual. Agreement to V-Health Passport processing some specified classes of personal data is a condition of employment for staff.
- V-Health Passport may process sensitive information about a person's health, disabilities, criminal convictions, race or ethnic origin in pursuit of the legitimate interests of V-Health Passport. V-Health Passport may also require such information for the administration of the sick pay policy, the absence policy or the equal opportunities policy, or for internal review.
- V-Health Passport may also ask for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. V-Health Passport will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency. The consent of the data subject will always be sought prior to the collection of any sensitive data.

The Data Controller and the Designated Data Controllers

The V-Health Passport Board of Directors and Management is the data controller. Responsibility for day-to-day matters will be delegated to the Heads of Department as designated data controllers. Information and advice about the holding and processing of personal information is available from the Director.

Retention of Data

V-Health Passport will keep different types of information for differing lengths of time, depending on legal and operational requirements. These requirements are described in Information Audit Policy.

Removal of Data

A data source can request the removal of data from our information collections. However, depending on the type of data being requested to be deleted, this will be carried out in accordance with regulatory and legislative restraints.

Employment Data

Employment data is required to be retained for 3 years after employment. Therefore, all data will automatically be deleted after this time period. A request to delete this data will therefore be delayed until this time period has been reached.

Financial Data

Financial data is required to be retained for a minimum period of 7 years. Therefore, all financial data pertaining to the data source will be deleted from logical systems after this time period.

Compliance

- Compliance with Data Protection is the responsibility of members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Director.
- Any individual, who considers that the policy has not been followed in respect of personal data about him or herself, should raise the matter with the designated data controller initially. If the matter is not resolved, it should be referred to the staff grievance or complaints procedure.

Data Security

Whether end users are using desktop or laptop PCs, there is a risk that data can be lost due to hardware failure or user error. Staff must accept responsibility for the machines they use to ensure that data is regularly backed up to minimise loss to the business as a result of such events. In particular, care of customer data must be taken very seriously.

You should only take data sufficient for your need

- You should only hold data for the minimum time required to complete your work
- You should destroy data when no longer required and confirm to the client this has been done
- Where classified information must be processed on a portable computer in an area where not all personnel are cleared or have a "need to know", position the computer carefully to avoid casual overview.
- Products for secure access control and hard-disk encryption are recommended for laptops that contain classified information and may be taken outside the organisation. V-Health Passport already employs software to carry this out and where is deemed necessary these measures are in place.

Data Protection Controls

As V-Health Passport is considered a processor of external data and the controller of internal data, the GDPR places specific legal obligations; e.g. requirement to maintain records of personal data and processing activities. There will be more legal liability if V-Health Passport are responsible for a breach.

Data breaches are managed as per the Information Security Incident Policy, however if a breach is considered notifiable V-Health Passport must report the breach within 72 hours of being aware of it. Notification to the relevant supervisory authority is only necessary where there is likely to be risk to the rights and freedoms of individuals.

Our Privacy Statement is published to our website. All information collections have been identified and have undergone a Data Protection Impact Assessment (DPIA).

The following documents can be used to confirm compliance:

- Back Up Policy
- Information Audit Policy
- Information Security Incident Policy
- Malware Protection Policy
- Subject Access Request Policy
- DPIA – ISOrisk