Data Protection & Security Policy

This is the statement of general policy and arrangements for:	Dhiverse Head Office, Dales Brewery, Gwydir Street, Cambridge, CB1 2LJ
Overall & final responsibility for ensuring this policy is put into practice is delegated to:	Renee West, Chair of Trustees
Day to day responsibility for ensuring this policy is put into practice is delegated to:	Sharron Spindler, Chief Executive Officer (CEO)

1. Introduction

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government, and is the UK's implementation of the General Data Protection Regulation (GDPR).

As an employer, registered charity and a provider of social care services, Dhiverse needs to collect and store certain information about its employees, trustees, volunteers and service users, including Personal Identifiable Data (PID). This allows us to monitor aims and objectives, outcomes and performance. It also enables us to ensure health and safety and safeguarding policies and procedures are followed and that the sharing of information, when requested and with consent, in order to ensure the best possible outcomes for service users and to meet all appropriate statutory requirements.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Dhiverse must comply with the strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race

- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

As a social care provider Dhiverse also works in line with the 6 Caldicott Principles, which are:

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law

Dhiverse employees, sessional workers and volunteers must follow these principles at all times.

The GDPR (General Data Protection Regulation) came into force on 25 May 2018. The regulation replaced the Data Protection Act 1998.

At Dhiverse, confidential means confidential to staff employed by Dhiverse, on a need to know basis. All Dhiverse staff sign the 'Managing Service User Information Guidelines'. Your information will be held securely and will not be divulged to anyone else other than for the reasons stated below.

Confidentiality cannot be assured where the following situations apply:

- If Dhiverse is obliged to disclose confidential information by a court order
- If a service user gives us information concerning abuse of a child

- If, by keeping confidentiality, a service user might suffer severe injury or abuse
- If, by keeping confidentiality, someone else might suffer severe abuse

Should any of the above arise then the Dhiverse representative should, where possible, advise the service user that they might need to break confidentiality, however it may be that the service user does not wish action to be taken; does not wish to become involved in an investigation and/or does not want confidential information to be shared with other individuals and agencies. In such a situation the Dhiverse representative should inform the service user that they have a duty to discuss the disclosure with an appointed person within Dhiverse and that the appointed person/s will decide whether the situation requires confidentiality to be broken. The appointed persons are the CEO or a person which this responsibility has been delegated to.

2. Purpose of the Policy

This Information Governance policy provides an overview of our organisation's approach to information governance; a guide to the procedures in use and details about the Information Governance management structures within the Organisation. The aim of the policy is to define the organization's commitment to having sound information governance arrangements in place and to give clear direction and guidance to staff and trustees whilst ensuring that legal requirements and best practice standards are met.

3. Our approach to Data Protection & Security

Our Organisations approach to implement data protection and security (information governance) effectively and to ensure the correct procedures are followed will require the following:

- Information will be protected against unauthorised access
- Information will be held securely
- Confidentiality will be assured
- Information will be complete, accurate and up to date
- Regulatory and legislative requirements will be met
- Training and guidance will be available to all staff and volunteers as necessary for their role
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated

4. Policies and Procedures in use in the organisation

This Data protection and security policy will be managed through staff and volunteer compliance with the following policies and procedures:

- Staff Compliance Guidance and Form for Confidentiality of Service Users
- HIV Policy
- Information Policy
- Confidentiality Policy
- Volunteer Policy
- Lone Working Policy
- Safeguarding Policy and Guidelines
- Compliance with the Data Protection Act

This policy is highlighted in Dhiverse's contract of employment. It also forms part of the staff induction process. Infringement of the requirements of this policy may result in disciplinary action being taken. If any Dhiverse staff, volunteers, members or service providers consider that this Policy has not been followed, in respect of personal data about themselves, they should raise the matter initially with the SIRO. If the matter is not resolved it should be raised as a formal grievance [see Grievance Policy]

Personal data is defined in the DPA 1998, at Section 1(1), as follows: *"data which relate to a living individual who can be identified from those data; or from those data and other information which is in the possession of, or is likely to come into the possession of, the Information Governance Lead and includes any expression of opinion about the individual and any indication of the intentions of the Information Governance Lead or any other person in respect of the individual".*

5. Staff training and guidance

Staff will receive the relevant training that is needed to adhere to our policies and procedures and will be provided with supplementary guidance where necessary. Compliance with the procedures will be monitored by the SIRO, and additional support and training will be provided where issues are identified.

6. Responsibilities and accountabilities

The Senior Information Risk Office (SIRO) and the Caldicott Guardian is Sharron Spindler, the CEO.

The key responsibilities of the SIRO are to:

- Oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the organisation's approach to information risk is effective, in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and / or discussion of information risk issues.
- Ensure the board is adequately briefed on information risk issues.
- Ensure that all care systems information assets have an assigned Information Asset Owner.

The organisation, through its CEO and Board of Trustees, is responsible for ensuring that sufficient resources are provided to support the effective implementation of IG to ensure compliance with the NHS information governance assurance framework.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of, and comply with, the requirements of this policy and the procedures and guidelines produced to support it. Where trained staff fail to adhere to the organisation's policy and procedures disciplinary action may be taken.

All staff are responsible for:

- checking that any information that they provide to Dhiverse in connection with their employment is accurate and up to date
- informing Dhiverse of any changes to information which they have provided, e.g. changes of address, contact number
- informing Dhiverse of any errors or changes in staff information

When, as part of their responsibilities, staff collect information (i.e. personal information, opinions about ability, or details of personal

circumstances) about other staff or service users, they must comply with any guidelines which may be published. In particular, they must seek the permission of the SIRO for their proposed information collection and uses.

The Chief Executive has overall responsibility and is responsible for monitoring the steps taken to ensure that the DPA 1998, the Caldicott Principles and this Policy are complied with. Particular care must be taken when work is being undertaken externally or when an existing body of data is being made available to Dhiverse for the first time.

Ensuring that they follow the 5 basic rules in respect of Data protection and security. At all times, information must be:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

7. Data security

Who is a service user? A 'service user' is anyone who uses our services.

We only hold limited data and information on service users where there is a need. Where we have had no contact from a service user for a **period of 6 months,** their file will be considered 'Inactive'. If after a **further 6 months** we have had no contact from the service user, their file will be shredded using a professional confidential waste company and electronic records will be permanently deleted. This means that no service user file will be kept for longer than **12 months after the last point of contact.** If a service user makes a request for their file to be destroyed sooner than that, then we will act on their request immediately. However, this request must be in writing.

How service user files are handled: Managers and the CEO will have access to service user files at all times. Other Dhiverse staff and volunteers are allowed access to a service user file for purposes of supporting the service user when support staff are unavailable and for reporting/safeguarding purposes as agreed with the CEO or delegated person. All service users, with a file, have the right to view their file. Files must be maintained in line with the Data Protection and Security Policy and must stored securely at all times on Dhiverse premises.

All computer records will be password protected and compliant with Dhiverse's IT security policy. No service user file should ever leave the Dhiverse office without the knowledge of the SIRO or delegated person.

Information held on a Dhiverse service user's hard copy file and electronic file is kept to a minimum, only relevant and factual information is recorded. If a service user provides copies of letters, forms etc. from e.g. NHS, HMRC, DWP for the purposes of support, this information will be shredded at the point it has been acted on and is no longer needed.

All staff are responsible for ensuring that:

- Any personal data, which they hold, or for which they are responsible, is kept securely, for example: kept in a locked filing cabinet or a locked drawer
- The key to the locked cabinet or drawer is kept in the key safe
- Electronic data is password protected
- Desktops and laptops are kept in suitably secure conditions and logged off and shut down when not in use
- Data should not be stored on the hard drives of desktop personal computers but on the networked storage facilities provided
- When doing outreach and home visits, if it is necessary to take paper files/information relating to the service user you are seeing, only the absolute essential paper information should be taken. This information must be transported in a Dhiverse black lockable briefcase and must not be taken on public transport. On returning to the office any paper information must be removed from the briefcase and returned to the locked cabinet or drawer immediately
- The clear desk procedure is followed before leaving the office i.e. no files or paperwork of a sensitive or confidential nature is left on the desk, drawers are locked and computers are shut down
- Where it is necessary to store information on laptop computers (on or off-site) then the laptop must at all times be maintained physically secure. Where the data is particularly sensitive, consideration must be given to the adoption of additional security measures which would protect the information in the event of the loss or theft of the computer. Care must be taken to ensure that data is frequently transferred to network storage and that discrepancies are not allowed to arise.
- Where information is to be gathered through, or used on, a website then appropriate measures must be in place to control access and prevent unauthorised disclosure

- Service users, read, understand and sign the information sharing agreement within the referral form before any support is given to said service user
- Service users receive a copy of the Information Handling Agreement at the first meeting

Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party; with the exception of vulnerable adults and children or others at risk. (See Safeguarding and Confidentiality Policies).

Advice on the collection, retention and secure storage of information may be obtained from the SIRO.

Staff should note that unauthorised disclosure is a breach of the DPA 1998 and may result in disciplinary action. In some cases it may be considered as gross misconduct. It may also result in a personal liability for the individual staff member.

8. Rights to access information (Subject Access Requests - S.A.R.s)

Employees and service users of Dhiverse have the right to access any personal data that is stored either on computer or in other types of files. Should any person wish to exercise this right they should contact the SIRO.

In order to gain access, where possible, a request should be made in writing. Dhiverse reserves the right to make a charge of up to £10 on each occasion that access is requested to cover admin costs. However a first request will usually be free of charge.

Dhiverse aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 20 working days.

9. Subject consent

GDPR states that: Processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing. Consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. In view of this Dhiverse will always ask or inform prospective staff, staff and service users that they need to collect certain data and why and obtain their consent where necessary.

10. Information sharing

At Dhiverse we aim to provide the best possible support to all our service users. At times, to ensure that a service user receives the best service and support to meet their needs it might be necessary for us to share relevant personal information with a third party agency. Our information sharing agreement is set out in our referral form and we would only ever share information with a third party with the signed consent of the service user. Third parties must agree to treat all information shared with them as confidential. The principles of information sharing are covered in our Confidentiality policy.

Exceptions to the principles outlined above might occur:

- If Dhiverse were to be obliged to disclose confidential information by a court order
- If a client were to give us information concerning abuse of a child
- If, by keeping confidentiality, a client might suffer severe injury or abuse
- If, by keeping confidentiality, someone else might suffer severe abuse (including death or serious injury through violence and/or sexual assault).

We would however, where possible, inform the service user of any situations where confidentiality might be broken without consent.

NB: Please refer to Dhiverse Safeguarding Policy in respect of the above points.

11. Processing sensitive information

In order for Dhiverse to meet its aims and objectives, and in particular, to ensure that our services reach seldom-heard and marginalized groups effectively, the organization needs to collect and store sensitive information about service users including ethnic identification, gender, sexuality, HIV status, other health/disabilities information and family details. It might also be necessary for Dhiverse to collect and process similar information from staff to ensure that Dhiverse can operate policies on matters such as sick pay, equal opportunities and ICE (in case of emergency) procedure. Dhiverse will only use such information in the protection of the health and safety of the individual, for example in the event of a medical emergency; but staff will need to have given prior consent to use this information for such an event. An exception would be

where there is a safeguarding issue when staff would need to inform the individual that they need to share information and the reason/s why, but consent does not need to be given.

Because this information is considered sensitive, and it is recognized that the processing of it may cause particular concern or distress to individuals, employees and others affected will be asked to give express consent for Dhiverse to collect this information.

12. Retention of data

The GDPR 2018 stipulates that data and records should only be stored for as long as they are useful, so it's up to the employer to determine how long those records are useful for. However it is recommended that personal information of employees, including contact details, appraisals, reviews, sickness etc.is kept for at least 5 years.

Retention of data follows statutory guidelines and best practice – in consequence different classes of data may be retained for varying periods.

Dhiverse will keep individual staff records or a period of 6 years after employment ceases**.** All Information will be stored securely. ***After 6 years*** all records and information will be shredded using a professional confidential waste company. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

Dhiverse will store service user files for ***1 year*** after last contact, unless we receive a request from the SU for the file to be destroyed. These files are archived and held securely in a locked room. However, with consent from the service user Dhiverse may keep service user name and basic contact details along with any other information the service user asks us to keep, for longer than 1 year so that the service user can receive pertinent update/event information. It is the service user's responsibility to advise us of any change to contact details.

Upon the conclusion of the retention period hard copy files and information are shredded and electronic information is deleted from the system.

Dhiverse will keep all financial records and information relating to Dhiverse as an organization **for a period of 7 years. After 7 years** all records and information will be shredded using a professional confidential waste company.

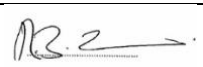
Information will be stored securely. This is in line with both:

- The Information Commissioners Office (ICO) rules which states information should be kept for 6 years
- HMRC requirements which is to keep financial records for a period of 7 years to cover all HMRC Enquiry time limits after the 6 years.

13. Conclusion

Compliance with the GDPR 2018 and the Caldicott Principles is the responsibility of all staff, volunteers, trustees and members of Dhiverse. Any deliberate breach of this policy may lead to disciplinary action being taken, or access to Dhiverse's facilities being withdrawn, expulsion from Dhiverse or a criminal prosecution.

Any questions or concerns about the interpretation or operation of this Policy should be taken up with the SIRO.

Signed (Employer)	Signature: 		Rob Turner, Chair	Introduced & Approved: May 2016
Responsible for policy review and update:	Sharron Spindler, CEO	Every:	**2 years** or sooner if work activity, a specific situation or legislation dictate that a review is necessary/required	
How will the policy be reviewed:	At a staff meeting with the involvement of staff and volunteers. The reviewed and updated policy will be approved by the Board of Trustees.			
Date of next full review:	**February 2021**			
Revised: 12 February 2019	 on behalf of the board		12 March 2019	