Data Protection Policy

Document Control		Applicable To:	All Staff
Version Number:	3	Previous Version No.:	2
Date Drafted:	May 2018	Next Review Date:	May 2021
Responsible Officer:	Data Protection Officer	Approved by Committee:	
Approved by Board (if relevant): 25/05/2018			
Date Equality Impact Assessed:			

1. Introduction

1.1. In order to operate effectively, Trivallis gathers, holds and processes personal data about its employees and employment applicants, non-executive directors, volunteers and trainees, tenants, leaseholders, customers, contractors and suppliers.

1.2. This data must be processed in accordance with the requirements of the relevant data protection legislation which, from 25th May 2018, is the General Data Protection Regulation (GDPR), and in line with Trivallis' policies and procedures.

1.3. Trivallis will comply with the performance standards as set out in the Welsh Government Regulatory Framework.

2. Policy statement

2.1. Trivallis, acting as a controller, recognises its legal and moral duty to ensure that personal data are handled properly at all times, irrespective of the format in which they are held. This covers the entire lifecycle of the data, including: -

- The obtaining of personal data;
- The storage and security of personal data;
- The use of personal data; and
- The disposal/destruction of personal data.

2.2. Trivallis regards the lawful and correct treatment of personal data as very important to its successful operations and to maintaining confidence between Trivallis and those with whom it carries out business.

2.3. Trivallis considers the rights of the individual, as outlined in the GDPR, to be fundamental and will ensure that these rights are upheld.

3. Policy aims

3.1. This policy aims to ensure that effective rules are adopted for the efficient management and administration of Trivallis, both now and in the future.

3.2. This policy aims to protect and promote the rights of individuals and Trivallis and to ensure compliance with the relevant data protection legislation by ensuring that individuals who process personal data for or on behalf of Trivallis are aware of, and understand the importance of data protection and the requirements of the relevant data protection legislation.

4. Scope

4.1. The scope of this policy extends to all Trivallis' departments, employees, non-executive directors, data processors and third parties who process personal data on behalf of Trivallis.

4.2. All individuals will ensure that they are aware of, and adhere to, Trivallis' policies and procedures regarding the processing of personal data and that all personal data ara processed in accordance with the requirements of the relevant data protection legislation.

5. Key definitions

5.1. Personal data

5.1.1. Personal data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This includes, but is not limited to name, address, date of birth, contact details and IP address.

5.2. Sensitive personal data

5.2.1. The GDPR refers to sensitive personal data as 'special categories of personal data'.

5.2.2. The special categories specifically include race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

5.2.3. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

5.2.4. Personal and sensitive personal data could relate to Trivallis':

- Customers (tenants and applicants for housing);
- Clients (organisations or persons to whom we provide a service);
- Suppliers and partners (contractors, local authorities and stakeholders); or
- Non-executive directors, employees and volunteers.

5.3. Controller

5.3.1. A controller determines the purposes and means of processing personal data.

5.4. Processor

5.4.1. A processor is responsible for processing personal data on behalf of a controller.

5.5. Data subject

5.5.1. A data subject is a natural person whose personal data is processed by a controller or processor.

5.6. Third party

5.6.1. A third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

5.7. Recipient

5.7.1. A recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

5.8. Processing

5.8.1. Processing is any operation performed on personal data, whether or not by automated means, including collection, recording, use, storage, erasure or destruction etc..

6. Data protection principles

6.1. The GDPR is underpinned by a number of data protection principles, contained in Article 5, which set out the main responsibilities for organisations processing personal data.

6.2. Trivallis, as a controller, is responsible for, and must be able to demonstate compliance with, these principles. These principles are:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

6.3. See Appendix 1 for details of the GDPR data protection principles.

7. Lawfulness of processing personal data

7.1. Processing personal data lawfully as required by the first principle of the GDPR, requires a lawful basis under Article 6. Processing sensitive personal data lawfully requires a lawful basis under Article 6 and a separate condition under Article 9. Also, in order to comply with the accountability principle in Article 5, a controller must be able to demonstrate that a lawful basis applies.

7.2. The lawful basis for processing must be determined and documented before the processing begins.

7.3. The lawful bases that Trivallis relies upon to process personal data are detailed in Trivallis' Information Asset Policy and Register. The lawful bases for processing personal data are:

- Consent;
- Contractual necessity;
- Compliance with legal obligation;
- Vital interests;
- Public interest; and
- Legitimate interests.

7.4. The lawful bases for processing sensitive personal data are:

- Explicit consent;
- Employment law;
- Vital interests;
- Charity or not-for-profit bodies;
- Data manifestly made public by the data subject;
- Legal claims;
- Reasons of substantial public interest;
- Medical diagnosis and treatment; and
- Public health;
- Historical, statistical or scientific purposes.

7.5. See Appendix 2 for details of the lawful bases for processing personal and sensitive personal data.

8. Rights of the individual

8.1. Under the GDPR, an individual has a number of rights with regards to a controller and Trivallis will ensure that, with regard to the processing of personal data, these rights are upheld. These right are:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights related to automated decision making including profiling.

8.2. See Appendix 3 for details of the rights of the individual.

9. Roles and responsibilities

9.1. Everyone who works for or with Trivallis has a responsibility for ensuring that personal data are collected, stored, handled and disposed of appropriately.

9.2. Each team that handles personal data must ensure that it does so in line with this policy and with the principles of the relevant data protection legislation:

9.2.1. **Trivallis Ltd**

With regard to the personal data that Trivallis processes, Trivallis is the controller.

9.2.2. **The Board**

Will have overall accountability and responsibility for ensuring that Trivallis meets its legal obligations.

9.2.3. **The Data Protection Officer**

Will:

- Keep Trivallis updated about its data protection responsibilities;
- Review all data protection procedures and policies in line with an agreed schedule;
- Arrange data protection training and advice for the company;

- Provide guidance on the processing of personal data and handle questions from Trivallis' data subjects;
- Deal with requests from data subjects for access to their information;
- Deal with data breaches; and
- Coordinate data protection impact assessments.

9.2.4. **The Information Governance Forum**

Will co-ordinate responsibility for the processing of personal data by promoting awareness throughout the business, and assisting with investigations into data breaches or loss of personal and sensitive personal data.

9.2.5. **All employees, data processors and third parties**

All employees, data processors and third parties will ensure that they are aware of, and adhere to, Trivallis' policies and procedures regarding the processing of personal data and that all Trivallis' personal data is processed in accordance with the requirements of the relevant data protection legislation.

10. General staff guidelines

10.1. Employees should only be able to access the personal data that they require in order to do their work.

10.2. Personal data should not be shared informally between employees – when access to personal data is required, employees can request it from their line managers.

10.3. Trivallis will provide training to all employees to help them understand their responsibilities when handling personal data.

10.4. Employees should keep all personal data secure by taking sensible precautions.

10.5. Strong passwords must be used on IT equipment and they should never be shared.

10.6. Personal data should not be disclosed to unauthorised people, either within the company or externally.

10.7. Personal data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

10.8. Employees should request help from the Data Protection Officer if they are unsure about any aspect of data protection.

11. Training

11.1. All employees responsible for handling personal data will receive training, and it will be included as part of the induction programme for new employees who are required to handle personal data.

11.2. All employees will ensure that they complete all mandatory data protection training.

11.3. Any breach of data protection legislation or this policy by employees will be dealt with under the Disciplinary Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

12. Data collection

12.1. Trivallis will not attempt to gain access to personal data that it is not necessary for it to hold. All personal data held will be relevant to the purpose for which it is required and will be held and processed in accordance with the requirements of the relevant data protection legislation.

13. Data storage

13.1. Trivallis will take steps to ensure that personal data are kept secure at all times against unauthorised or unlawful processing and against accidental loss, destruction or damage. Questions about storing personal data safely should be directed to the Data Protection Officer.

13.2. The following guidelines apply to personal data that is stored either electronically or as hard copy (on paper):

- When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it;
- When not required, the paper or files should be kept in a locked drawer or filing cabinet;
- Employees should ensure that paper and printouts are not left where unauthorised people could see them, like on a printer;
- Personal data stored on paper should be shredded and disposed of securely when no longer required;
- When personal data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts;
- Personal data should be protected by strong passwords that are changed regularly and never shared between employees;
- If personal data are stored on removable media (like a CD or USB memory stick), these should be encrypted and kept locked away securely when not being used;

- Personal data should only be stored on designated drives and servers;
- Servers containing personal data should be sited in a secure location, away from general office space;
- Personal data should be backed up frequently. Those backups should be tested regularly, in line with the Trivallis' standard backup procedures;
- Personal data should never be saved directly to laptops or other mobile devices like tablets or smart phones; and
- All servers and computers containing personal data should be protected by approved security software and a firewall.

14. Data use

14.1. Personal data are of no value to Trivallis unless the business can make use of them. However, it is when personal data are accessed and used that they can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended;
- Personal data should not be shared informally. In particular, they should never be sent by unsecure email;
- Personal data must be encrypted before being transferred electronically outside of the company. Trivallis' IT Helpdesk can explain how to send personal data securelty to authorised external contacts;
- Personal data should never be transferred outside of the European Economic Area without first seeking guidance from the Data Protection Officer; and
- Employees should not save copies of personal data to their own computers - always access and update the central copy of any data.

15. Data accuracy

15.1. The law requires Trivallis to take reasonable steps to ensure that personal data are kept accurate and up to date. The more important it is that the personal data are accurate, the greater the effort Trivallis should put into ensuring accuracy.

15.2. It is the responsibility of all employees who work with personal data to take reasonable steps to ensure that the data are kept as accurate and up to date as possible.

15.3. Personal data will be held in as few places as necessary. Employees should not create any unnecessary additional datasets.

15.4. Employees should take every opportunity to ensure that personal data are kept updated. For instance, by confirming a customer's details when they call.

15.5. Personal data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

16. Providing information to the data subject

16.1. In accordance with the requirements of the GDPR, Trivallis aims to ensure that individuals are aware that their personal data is being processed and that they understand:

- Who the controller is;
- Why we process their personal data;
- What personal data we process and where we get it from;
- Who we share their personal data with;
- Whether we transfer their personal data outside of the European Economic Area;
- How long we hold their personal data for;
- What rights they have.

16.2. This information is provided to the data subject in an information notice, and copies of Trivallis' information notices can be found on Trivallis' website.

17. Disclosing personal data for other reasons

17.1. In certain circumstances, the GDPR allows personal data to be disclosed to third parties without the consent of the data subject. The Data Protection Officer must be contacted before any data are disclosed to a third party.

18. Personal data breaches

18.1. Article 5 of the GDPR requires that personal data must be processed in a manner that ensures appropriate security.

18.2. A personal data breach means 'a breach of security leading to the accidental destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

18.3. It is the responsibility of all staff to inform Trivallis' Data Protection Officer when they are made aware of a personal data breach. The Data Protection Officer will then take the appropriate action in accordance with the requirements of Trivallis' Data Breach Notification Procedure.

19. Subject access requests

19.1. All individuals who are the subject of personal data held by Trivallis are entitled to obtain:

- Confirmation that their personal data are being processed;
- Access to their personal data; and
- Other supplementary information corresponding to the information that should be provided in a privacy notice e.g. information about the source and recipients of the data, information about the envisaged retention period of the data, details of any international transfers involving the data, and details of the right to have inaccurate data corrected and to lodge a complaint with a supervisory authority.

19.2. If an individual contacts the company requesting this information, this is called a subject access request.

19.3. Subject access requests from individuals should be forwarded immediately to the Data Protection Officer, who will process the request in accordance with Trivallis' Right of Access Procedure.

20. Retention

20.1. The GDPR's principle of storage limitation says that '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 are processed', and Trivallis will ensure that personal data are deleted in accordance with the requirements of this principle and in line with the Data Retention Policy and Register.

20.2. Where, due to software constraints, we have to hold personal data for longer than is specified in the Data Retention Policy and Register, Trivallis will look to anonymize it.

21. Disposal of personal data

21.1. Where personal data are no longer required, they will be destroyed in accordance with the requirements of the relevant data protection legislation.

22. Monitor and review

22.1. This policy will be reviewed every three years to ensure that it is effective and complies with the relevant data protection legislation and current good practice. A review will be carried out sooner should there be any changes to statutory requirements.

23. Equal Opportunities

23.1. No adverse consideration will be given to race, ethnic origin, nationality, religion, cultural background, gender, sexual orientation, domestic circumstances, disability, illness (such as HIV and Aids) or age.

24. Complaints

24.1. If a person has cause to believe that Trivallis has failed to meet its commitments within this policy, they should complain to the Data Protection Officer or the Information Commissioner's Office.

25. Linked Policies

- Information Asset Policy and Register
- Data Retention Policy and Register
- Data Breach Notification Procedure
- Data Protection Impact Assessment Procedure
- Processing Personal Data With Consent Procedure and Register
- Right of Access Procedure
- Third Party Data Sharing Procedure and Register

Appendix 1

The GDPR requires controllers to embed six privacy principles within their operations:

Lawfulness, fairness and transparency

Personal data must be processed lawfully, faily and in a transparent manner in relation to the data subject.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatable with those purposes.

Data minimisation

Personal data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are processed.

Accuracy

Personal data must be accurate and, where necessary, kept up to date.

Storage limitation

Personal data must 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 are processed.

Integrity and confidentiality

Personal data must 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, using appropriate technical or organisational measures.

Accountability

In addition to the above, the controller shall be responsible for, and be able to demonstrate compliance with, these principles.

Appendix 2

Processing shall be lawful only if and to the extent that at least one of the following applies:

Lawful bases for processing personal data

Consent

The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Contractual necessity

Processing is necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract.

Compliance with legal obligation

Processing is necessary for compliance with a legal obligation to which the controller is subject.

Vital interests

Processing is necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent.

Public interest

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 controller.

Legitimate interests

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Lawful Bases for Processing Special Categories of Personal Data

The following categories of personal data are considered 'sensitive':

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data concerning health or sex life or sexual orientation;

- Genetic data; and
- Biometric data where processed to uniquely identifying a natural person

Explicit consent

The data subject has given explicit consent, unless reliance on consent is prohibited by EU or member state law.

Employment law

Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.

Vital interests

Processing is necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent.

Charity or not-for-profit bodies

Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

Data manifestly made public by the data subject

Data manifestly made public by the data subject.

Legal claims

Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

Reasons of substantial public interest

Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures.

Medical diagnosis and treatment

Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with health professiona; and

Public health

Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

Historical, statistical or scientific purposes

Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Appendix 3

Under the GDPR, the Rights of the Individual are:

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

Controllers must provide individuals with information including the purposes for processing their personal data, the retention periods for that personal data, and who the data will be shared with. This is called privacy information. Privacy information must be provided to individuals at the time that the controller collects their personal data from them.

Right of access

Individuals have the right to access their personal data.

Refer to Trivallis' Right of Access procedure for further details.

Right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

Right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'.

Right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

Right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Right to object

The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances

Rights related to automated decision making including profiling

The GDPR has provisions on:

Automated individual decision-making (making a decision solely by automated means without any human involvement); and

Profiling (automated processing of personal data to evaluate certain things about an individual).

Profiling can be part of an automated decision-making process.