



Telford and Wrekin

CVS

Involving, Inspiring, Supporting

Data Retention Policy (GDPR)

9 February 2022

CONTENTS

1. INTRODUCTION	2
2. AIMS AND OBJECTIVES.....	2
3. SCOPE	3
4. DATA SUBJECT RIGHTS AND DATA INTEGRITY.....	3
5. TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES.....	3
6. DATA DISPOSAL.....	5
7. DATA RETENTION	5
8. ROLES AND RESPONSIBILITIES.....	6
9. IMPLEMENTATION OF POLICY.....	6
10. RETENTION TIMETABLE GUIDELINES.....	7

1. INTRODUCTION

This Policy sets out the obligations of **Telford & Wrekin CVS whose** registered office is at **Suite 12 & 15 Hazledine House, Central Square, Telford Centre, Telford, Shropshire, TF3 4JL** (“the Company”) regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data has to be erased to comply with a legal obligation; or
- f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company’s Data Protection Policy.

2. AIMS AND OBJECTIVES

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. SCOPE

3.1 This Policy applies to all personal data held by the Company and by third-party data processors processing personal data on the Company's behalf.

3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:

- a) The Company's servers, located in Suite 12 & 15 Hazledine House, Central Square, Telford Centre, Telford, Shropshire, TF3 4JL
- b) Third-party servers, operated by Age UK and Landua located in Age UK Shropshire Telford & Wrekin, 3 Mardol Gardens, Shrewsbury, Shropshire SY1 1PR and Landau, 5 Landau Court, Tan Bank, Wellington, Telford, TF1 1HE
- c) Computers permanently located in the Company's premises at Suite 12 & 15 Hazledine House, Central Square, Telford Centre, Telford, Shropshire, TF3 4JL
- d) Laptop computers and other mobile devices provided by the Company to its employees;
- e) Computers and mobile devices owned by employees, agents, and sub-contractors;
- f) Physical records stored in CVS Offices at Suite 12 & 15 Hazledine House, Central Square, Telford Centre, Telford, Shropshire, TF3 4JL

4. DATA SUBJECT RIGHTS AND DATA INTEGRITY

4.1 All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.2 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, and further rights relating to automated decision-making and profiling.

5. TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Data Protection Policy for further details:

- a) All emails containing personal data must be encrypted;
- b) All emails containing personal data must be marked "confidential";
- c) Personal data may only be transmitted over secure networks;
- d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
- e) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- f) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using internal secured post boxes, or via the postal service, marked clearly with the recipient's name and marked 'confidential'.;
- g) All personal data transferred physically should be transferred in a suitable secured container.;
- h) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Debbie Gibbon, Data Controller

- i) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
- k) Personal data must be handled with care at all times and should not be left unattended or on view;
- l) Computers used to view personal data must always be locked before being left unattended;
- m) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the Data Controller and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
- n) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;
- o) All personal data stored electronically should be backed up twice daily at 12:00pm and 8:00pm with backups stored onsite. All backups are encrypted onsite & offsite. All backups should be encrypted; All data offsite is held in the UK. Remote access to the data is locked down to specific IP addresses
- p) All electronic copies of personal data should be stored securely using passwords and encryption;
- q) All passwords used to protect personal data should be changed regularly and must be secure;
- r) All CVS computers are protected by 2-factor authentication arrangement. All CVS staff and volunteers can only access data stored on a computer with passwords which will be issued to them. No IT system can be accessed without both passwords. Staff and volunteers are asked to memorise their passwords and must not record them anywhere.
- s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.;
- t) All software should be kept up-to-date. Security-related updates should be installed; All machines have a 3rd party patch management application that automatically scans and installs Microsoft updates that are deemed critical & important. This is the same for 3rd party software (Adobe, Java, Serif etc). Any none critical or important ones are rolled up into a monthly update
- u) No software may be installed on any Company-owned computer or device without approval; and
- v) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Data Controller to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer the Company's Data Protection Policy for further details:

- a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;
- b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;
- c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

- d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;
- e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;
- i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;
- j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. DATA DISPOSAL

6.1 Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- a) Personal data stored electronically (including any and all backups thereof) shall be deleted securely. This may on occasion be by using an external provider;
- b) Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely. This may on occasion be by using the external provider.
- c) Personal data stored in hardcopy form shall be shredded
- d) Special category personal data stored in hardcopy form shall be shredded

7. DATA RETENTION

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

- a) The objectives and requirements of the Company;
- b) The type of personal data in question;
- c) The purpose(s) for which the data in question is collected, held, and processed;
- d) The Company's legal basis for collecting, holding, and processing that data;
- e) The category or categories of data subject to whom the data relates.

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the

data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

8. ROLES AND RESPONSIBILITIES

8.1 The Company's Data Protection Officer is Debbie Gibbon, 01952 262066, debbie.gibbon@tandwcvcs.org.uk.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.

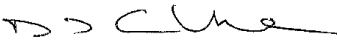
8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been reviewed, approved and authorised by:

Name:	Debbie Gibbon
Position:	CEO, Data Controller
Date:	9 February 2022
Due for Review by:	9 February 2023

Signature: 

10. RETENTION TIMETABLE GUIDELINES

Type of Employment Record	Statutory or Code of Practice Reference	Format and Location	Retention Period or Recommendation
Job applications and interview records of unsuccessful candidates	The Information Commissioner: Employment Practices Code Part 1: recruitment and selection (1.7.5)	Paper or electronic	A short period, perhaps 6 months after notifying unsuccessful candidates (or longer, if there is a clearly communicated policy to keep candidates CVs for future reference).
Personnel and training records	N/A	Paper or electronic	While employment continues and up to six years after employment ceases
Written particulars of employment, contracts of employment, and changes to terms and conditions	N/A	Paper or electronic	While employment continues and up to six years after employment ceases
Working time opt-out forms	<i>Regulations 5 and 9, Working Time Regulations 1998 (SI 1998/1833) (WTR 1998)</i>	Paper or electronic, originals are not required by the <i>WTR 1998</i>	Two years from the date on which they were entered into
Records to show compliance with the <i>Working Time Regulations 1998</i>	Regulations 5, 7 and 9, <i>WTR 1998</i>	Paper or electronic	Two years after the relevant period
Annual leave records	N/A	Paper or electronic	Six years or possibly longer if leave can be carried over from year to year
Payroll and wage records for unincorporated businesses	section 12B, Taxes Management Act 1970	Paper or electronic	Five years after 31 January following the year of assessment
Payroll and wage records for companies	Schedule 18, <i>paragraph 21, Finance Act 1998</i>	Paper or electronic	Six years from the financial year-end in

			which payments were made
PAYE records	<i>Regulation 97, Income Tax Regulations 2003</i>	Paper or electronic	Not less than three years after the end of the tax year to which they relate. However it may be sensible to keep them for six years as they may fall within the definition of payroll and wage records (see above)
Collective workforce agreements and past agreements that could affect present employees	N/A	Paper or electronic	Permanently
Works Council minutes	N/A	Paper or electronic	Permanently
Maternity records	<i>Regulation 26, Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)</i>	Paper or electronic	Three years after the end of the tax year in which the maternity pay period ends
Current bank details	N/A	Paper or electronic	No longer than necessary
Record of advances for season tickets and loans to employees	N/A	Paper or electronic	While employment continues and up to six years after repayment
Death Benefit Nomination and Revocation Forms	N/A	Paper or electronic	While employment continues or up to six years after payment of benefit
Any reportable accident, death or injury in connection with work	<i>Schedule 1, Part II, Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (SI 2013/1471)</i>	Paper or electronic	For at least three years from the date the report was made

Records in relation to hours worked and payments made to workers	<i>Section 9, National Minimum Wage Act 1998.</i> <i>Regulation 59, National Minimum Wage Regulations 2015 (SI 2015/621)</i>	Paper or electronic	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends
Consents for the processing of personal and sensitive data	<i>Schedule 1, DPA</i>	Paper or electronic	For as long as the data is being processed and up to 6 years afterwards
Disclosure and Barring Service (DBS), formerly Criminal Records Bureau (CRB), checks and disclosures of criminal records forms	ROA and Information Commissioner's Employment Practices Code Part 1.7.4 and 2.15.3	Paper or electronic	Should be deleted following recruitment process unless assessed as relevant to ongoing employment relationship. Once the conviction is spent, should be deleted unless it is an excluded profession
Immigration checks	<i>Immigration, Asylum and Nationality Act 2006</i>	Paper or electronic	Two years after the termination of employment