Woking Community Transport
Data Retention Policy

Introduction

This Policy sets out the obligations of Woking Community Transport (WCT), whose registered office is at Red House, Cemetery pales, Woking. GU24 0BL regarding retention of personal data collected, held, and processed by WCT 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 WCT 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;

This Policy sets out the type(s) of personal data held by WCT for the legitimate business of a recruitment agency, 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.

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 WCT 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 WCT, 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 WCT and by third-party data processors processing personal data on WCT's behalf.

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

a) Third-party servers.

b) Laptop computers and other mobile devices provided by WCT to its employees;

c) Computers and mobile devices owned by employees, agents, and subcontractors used in accordance with WCT's Data Protection and IT Security Policy;

d) Physical records stored in the Society's address

e) Employees and contractors under contract to WCT may temporarily store physical records off site in accordance with the WCT Data Protection and IT Security Policy.

4. **Data Subject Rights and Data Integrity**

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

4.1 Data subjects are kept fully informed of their rights, of what personal data WCT holds about them, how that personal data is used as set out in WCT's Data Protection Policy, and how long WCT 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).

4.2 Data subjects are given control over their personal data held by WCT 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 WCT's use of their personal data, and further rights relating to automated decision-making and profiling, as set out in WCT's Data Protection Policy.

5. **Technical and Organisational Data Security Measures**

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

a) Where possible all emails containing personal data should be sent encrypted;

b) All emails containing sensitive 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 transferred in hardcopy form, it should be passed directly to the recipient or sent using Royal Mail Special Delivery or Recorded Delivery;

f) All personal data transferred physically should be transferred in a suitable container marked “confidential”;

g) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from WCT’s DPM.

h) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

i) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of WCT or not, without authorisation;

j) Personal data must be handled with care at all times and should not be left unattended or on view;
k) Computers used to view personal data must always be locked before being left unattended;

l) 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 WCT where the party in question has agreed to comply fully with WCT’s Data Protection Policy and the GDPR;

m) All electronic copies of personal data should be stored securely using passwords and encryption;

n) All passwords used to protect personal data should be changed regularly and must be secure;

o) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method;

p) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

q) No software may be installed on any WCT owned computer or device without approval; and

r) Where personal data held by WCT is used for marketing purposes, it shall be the responsibility of the Finance and Administration Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out.

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

a) All employees and other parties working on behalf of WCT shall be made fully aware of both their individual responsibilities and WCT's responsibilities under the GDPR and under the WCT's Data Protection Policy;

b) Only employees and other parties working on behalf of WCT that need access to, and use of, personal data in order to perform their work shall have access to personal data held by WCT;

c) All employees and other parties working on behalf of WCT handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of WCT handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of WCT 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 WCT handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of WCT handling personal data will be bound by contract to comply with the GDPR and the WCT's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of WCT handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Society arising out of the GDPR and the WCT's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of WCT handling personal data fails in their obligations under the GDPR and/or the WCT's Data Protection Policy, that party shall indemnify and hold harmless WCT against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. **Data Disposal**

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:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely

6.2 Personal data stored in hardcopy form shall be shredded using a secure destruction recycling company and recycled. Certificates are issued and retained to confirm this action.

6.3 Special category personal data stored in hardcopy form shall be shredded using a secure destruction recycling company and recycled. Certificates are issued and retained to confirm this action.

7. **Data Retention**

7.1 As stated above, and as required by law, WCT 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 We will retain personal information for as long as necessary to fulfil the legitimate business purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of personal date, the purposes for which we process personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

7.3 In some circumstances we may anonymise personal information so that it can no longer be associated with an individual, in which case we may use such information without further notice to the individual.

7.4 Refer to schedule below for specific data retention timelines and disposal methods.

8. **Roles and Responsibilities**

8.1 WCT's Data Protection Manager (DPO), Neal Glass, Fleet Manager, 01483 744809 or email neal.glass@wokingbustler.org.uk.

8.2 The DPO shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, WCT'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 DPO shall be directly responsible for ensuring compliance with the above data retention periods throughout the Society.

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

9. Implementation of Policy, This Policy (revised) shall be deemed effective as of 25th March 2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Data Retention Schedule

Description of Data	How data held	Length of Retention	Method of Disposal
Passenger Records	Daily Hard Copies	1 day	Shredding
Passenger Records	Digitally on CATSS	5 years	Data Anonymised
Bank statements			
Contracts			
Petty Cash			
Annual Accounts			
Board meeting notes			
Payroll records			
Staff records			
Accident reports			
Occurrence reports			
Emails			
Insurance schedules			

WCT policy name:	**Data Retention**
Version:	**March 2022**