

# WWA Data Protection Policy

---

## Contents

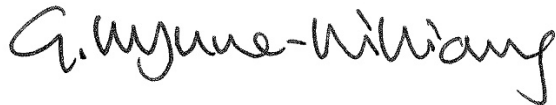
1	Introduction.....	3
2	Data Protection Act Registration .....	3
3	GDPR Compliance – Personal Data.....	3
3.1	<i>Staff Personal Data</i> .....	3
3.2	<i>Third Party Personal Data</i> .....	4
3.2.1	<i>Limitation</i> .....	4
3.2.2	<i>Business Contacts</i> .....	4
3.2.3	<i>Consultation Work</i> .....	4
4	Non-Personal Commercially Sensitive Data .....	4
5	Responsibilities for Handling Sensitive Data.....	5
6	IT Security.....	5

## Version Control

Version	Author	Changes from previous version	Checked by	Date checked
01	MM	None	GW	27 Apr 18
02	MM	Revised to note use of Xero accounts program with effect from April 2019 and to expand policy to cover non-personal commercially sensitive data.	GW	2 May 19
03	FE	None	GW	6 Sept 21

## 1 Introduction

- 1.1 This policy has been drawn up following a review by director and office manager M McGrath of the implications of the GDPR regulations for Wynne-Williams Associates Ltd ("WWA").
- 1.2 This policy is reviewed periodically and where there is any relevant change in the law or in the company's procedures and activities.
- 1.3 This version of the WWA data protection policy has been reviewed and signed off by:



Gill Wynne-Williams  
Managing Director  
September 2021

## 2 Data Protection Act Registration

- 2.1 WWA is registered with the Information Commissioner's Office (reference Z131542X). This registration renews annually. It is the responsibility of the office manager to ensure that the terms of this registration including the description of the types of data processing carried out by the company is accurate.

## 3 GDPR Compliance – Personal Data

### 3.1 Staff Personal Data

- 3.1.1 Like all businesses we keep some personal employee data for tax or employment law reasons: date of birth, sickness records, NI numbers, private addresses. This is kept on a restricted drive on the server accessible only by the directors, and on the accounts program Xero. This is a cloud-based system which is certified ISO/IEC 27001:2013 compliant (an international standard of data security). Director Matt McGrath and the administrative assistant are the only ones with access to this program and the data it holds.
- 3.1.2 The holding of such information is lawful under GDPR as being necessary to meet legal obligations. All those with access to this data are aware of their duty not to disclose to third parties and this is set out in the Staff Handbook.
- 3.1.3 We have obtained consent from all relevant staff to keep copies of their DBS (Disclosure and Barring Service) certificates to make it easy to send copies to schools etc that demand to see them. These are kept on a secure area of the server accessible only to directors. Staff are entitled to ask the company to delete their DBS records at any time.
- 3.1.4 The personal data of ex-employees needed to meet tax law requirements is retained securely for 6 years after they leave. DBS certificates are deleted as soon as the individual leaves employment.

- 3.1.5 All staff are told of the holding of their personal data by the company and they may see a copy of this data upon request. This is set out in the Staff handbook.

## 3.2 Third Party Personal Data

### 3.2.1 Limitation

- 3.2.1.1 It is company policy to limit the processing of third party personal data solely to the scenarios described below. The Staff Handbook sets out that staff should not undertake work which involves the processing of personal data for other purposes without prior agreement by a director. This agreement will only be given if a process can be defined that ensures that GDPR rules have been met.

### 3.2.2 Business Contacts

- 3.2.2.1 Staff have been instructed on keeping only business-relevant personal data about work contacts on the company's systems (principally in their Outlook address books and email inboxes). This is to ensure that this data is being held under a lawful basis of legitimate interest. This is set out in the Staff Handbook.

### 3.2.3 Consultation Work

- 3.2.3.1 We are occasionally required by our clients to carry out consultation exercises with members or the public or with individuals with an interest in a proposed development.
- 3.2.3.2 Our policy in such cases is to discuss with the client first whether any **personal data** needs to be collected in such exercises. For example, questionnaires which are anonymous, or which don't seek information which can be linked to an individual, do not collect personal data. **Data protection legislation does not apply if the data is not personal.**
- 3.2.3.3 If the client does require us to collect personal data on our behalf then we have defined processes (see separate documentation) for these exercises that ensure that we are holding any personal data only by consent, in secure form, and that we have met GDPR requirements on the right to be informed and retention/deletion.

## 4 Non-Personal Commercially Sensitive Data

- 4.1 The GDPR does not apply to data which is not personal. However, WWA also holds data which although not personal is commercially sensitive.
- 4.2 Where this data belongs to WWA itself (eg its own accounts) then:
- The Staff Handbook sets out the duty that all staff with access to this data have not to disclose to other parties without consent of the directors
  - The accounts information is primarily held in Xero, a cloud-based system which as noted above meets current international data security standards.
- 4.3 WWA staff may from time to time be provided with commercially sensitive data by clients. Tender or bid information, for example. In all cases the lead WWA employee for the project or client is required to confirm with the client what arrangements they require with respect to protection of such information and arrangements for its deletion. If required these can include restriction of access to any such information held

on WWA's server to named individuals using a protected subfolder or password protection on individual files.

- 4.4 The company has a shredder which is to be used for destroying paper copies of sensitive data.

## 5 Responsibilities for Handling Sensitive Data

- 5.1 The managing director has ultimate responsibility for ensuring that the company and its employees adhere to the law and to this policy in handling personal or commercially sensitive data.
- 5.2 Director M McGrath (office manager) is responsible for day to day monitoring, checking and updating of this policy, the relevant parts of the staff handbook, and the relevant procedures.
- 5.3 All staff are responsible for maintaining the security of sensitive data that they have access to in the course of their duties and for following the procedures in the Staff Handbook to prevent unauthorised access and otherwise to comply with legal requirements. Breach of the Staff Handbook requirements on data security is subject to disciplinary action which may result in dismissal.

## 6 IT Security

- 6.1 Access to the WWA server is restricted to WWA staff by domain password. Our password policy is:
- Users are required to change password every 6 months
  - Password must be at least 8 characters long and contain at least 1 uppercase, one number and one special character.
- 6.2 Remote access to the server is controlled by a VPN system running on a virtual machine on the main server. VPN remote access is limited to certain individual users with work laptops and all VPN data is encrypted.
- 6.3 All computers attached to the WWA network run eSet anti-virus software. All the office-based PC also run Heimdal Thor software which prevents links to untrusted websites being accessed.
- 6.4 Physical access to the server is protected by the same burglar alarm system as the rest of the office.