DATA PROTECTION POLICY

Robert Walpole and Partners
10 Banbury Avenue
Slough, Berkshire
SL1 4LH
Tel.: (01753) 530836

E-mail: admin@rwalpole.globalnet.co.uk

CONTENTS

REVISION TABLE 2

1. DATA PROTECTION POLICY STATEMENT 3

2. POLICY SCOPE 4

3. WHAT INFORMATION IS COLLECTED AND LAWFUL BASIS FOR ITS PROCESSING 5

4. DOCUMENT RETENTION TIMES 5

5. RESPONSIBILITIES 6

6. DATA SECURITY 7

7. DATA STORAGE 8

8. DATA USE 9

9. DATA ACCURACY 9

10. SUBJECT ACCESS REQUESTS 10

11. DISCLOSING DATA FOR OTHER REASONS 10

12. PERSONAL DATA BREACH 10

KEY

[A31] = Electronic Folder Reference

REVISION TABLE

Revision	Date	Comments
1	17/12/2015	First Issue
2	24/05/2018	Amendment for new GDPR 2018 regulations
3	09/07/2019	Periodic amendment
4	09/07/2020	Amendment to document retention times New guidance on confidential printouts when working remotely

1. DATA PROTECTION POLICY STATEMENT

Robert Walpole and Partners needs to gather and use certain information about individuals in order to perform its legal duties or satisfy contract requirements. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. Robert Walpole and Partners exercises overall control over the purposes and means of the processing of personal data and thus falls into 'controllers' category as defined by Data Protection Act 2018.

This policy describes how the personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

This data protection policy ensures Robert Walpole and Partners:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

Robert Walpole and Partners aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights in relation to data protection legislation.

Progress in implementing this policy will be reviewed annually by the partners.

Signed: M. J. Walpole.

M. J. Walpole
Partner

Date: 09.07.20

2. POLICY SCOPE

The Data Protection Act 2018 describes how organisations — including Robert Walpole and Partners — must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or by other means. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The current data protection regulations set out seven key principles. These say that personal data must:

1) Be processed fairly, lawfully and in transparent manner.
2) Be obtained and processed only for specific, lawful purposes.
3) Be adequate, relevant and not excessive.
4) Be accurate and kept up to date.
5) Not be held for any longer than necessary.
6) Be protected in appropriate ways.

And add that:

7) The controller shall be responsible for, and be able to demonstrate compliance with, the above principles ('accountability' principle).

More information can be found on government https://www.gov.uk/data-protection or Information Commissioner's Office website https://ico.org.uk/.

This policy applies to the head office, all staff and volunteers, all contractors, suppliers and other people working on behalf of Robert Walpole and Partners. It applies to all data that the company holds relating to identifiable individuals.

This policy helps to protect Robert Walpole and Partners from some very real data security risks, including:

a) Breaches of confidentiality. For instance, information being given out inappropriately.
b) Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
c) Reputational damage. For instance, loss of client's confidence if hackers successfully gained access to sensitive data.

3. WHAT INFORMATION IS COLLECTED AND LAWFUL BASIS FOR ITS PROCESSING

The below table outlines types of personal data that is collected by Robert Walpole and Partners and the lawful basis for processing this data.

Table 1: Types of data collected by Robert Walpole and Partners

Type of personal data	Example of data	Lawful basis for processing
Personal details	Name, date of birth, postal address, National Insurance number	Legal obligation (HMRC)
Personal contact details	E-mail address, telephone number(s), next of kin name and contact details	Consent
Proof of identity	Copy of passport or driving licence or acceptable equivalent	Legal obligation (checking person's right to work)
Proof of training	Copy of safety training certificates or cards	Legal obligation (Health and Safety)
Medical records (assessments or examinations)	Fitness for work assessment Drugs and alcohol testing Sickness records Medicals	Special category data
Financial data	Payroll details Pension details	Legal obligation (HMRC)
Other	Vehicle registration data Annual reviews Competency assessments Correspondence Curriculum Vitae	Legitimate interests

4. DOCUMENT RETENTION TIMES

Current data protection regulations in line with the minimisation and accuracy principles, impose data storage limitation. This means that personal data should not be kept for longer than it is required. Robert Walpole and Partners aims to erase or dispose of personal data within 3 months of the data subjects leaving the company unless the data falls into special category listed below.

Some documents need to be kept for longer due to specific requirements. These include but are not limited to:

a) payroll records need to be archived for a minimum of 3 years from the end of the tax year they relate to for HMRC auditing purposes (source: www.gov.uk; PAYE and payroll for employers);
b) pension schemes need to keep records for a minimum of six years (source: www.thepensionregulator.gov.uk; Keeping records);
c) copies of documents used for a right to work check should be kept securely for the duration of the worker's employment and for two years afterwards; The copy must then be securely destroyed (Home Office guidance 28 January 2019);
d) Results of Drug and Alcohol tests will be held on file for a minimum period of 10 years (from the date of the test); Records of positive tests shall be retained indefinitely (Sentinel Scheme requirement).

5. RESPONSIBILITIES

Everyone who works for or with Robert Walpole and Partners has some responsibility for ensuring data is collected, stored and handled appropriately. Each team member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Employees should request help from their immediate managers if they are unsure about any aspect of data protection.

The partners are ultimately responsible for ensuring that Robert Walpole and Partners meets its legal obligations. This may include:

a) Reviewing all data protection procedures and related policies, in line with an agreed schedule.
b) Arranging data protection training and advice for the people covered by this policy.
c) Handling data protection questions from staff and anyone else covered by this policy.
d) Dealing with requests from individuals to see the data Robert Walpole and Partners holds about them (also called 'subject access requests').
e) Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
f) Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
g) Performing regular checks and scans to ensure security hardware and software is functioning properly.

h) Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
i) Approving any data protection statements attached to communications such as emails and letters.
j) Addressing any data protection queries from journalists or media outlets like newspapers.
k) Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Personal data is processed primarily for secondary purposes (e.g. payroll or HR information) and is not part of carrying out Robert Walpole and Partners primary objectives. Therefore, no Data Protection Officer (DPO) needs to be appointed under the current data protection regulations.

6. DATA SECURITY

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees can request it from their immediate manager. Robert Walpole and Partners will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

a) Strong passwords must be used.
b) Personal data should not be disclosed to unauthorised people, either within the company or externally.
c) Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted or disposed of in appropriate manner (for instance shredded).

7. DATA STORAGE

These rules describe how and where personal data should be safely stored.

When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason. When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer. Data printouts should be shredded and disposed of securely when no longer required. Data printouts generated when working remotely should be safely stored until they can be brough into the office for filing or safe disposal (e.g. shredding).

When personal data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

a) Data should be protected by strong passwords that are changed regularly.
b) If data is stored on removable media, these should be kept locked away securely when not being used.
c) Data should only be stored on designated drives and servers, and should only be uploaded to approved cloud computing services.
d) Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
e) Data should not be saved directly to laptops or other mobile devices like tablets or smart phones.
f) All servers and computers containing data should be protected by approved security software and a firewall.

The above also applies in most cases to other data the company holds, including technical, commercial, and project specific data. However, in such cases all Robert Walpole and Partners staff have the ability to access the data through the internal server.

8. DATA USE

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

a) Personal data should not be shared informally.
b) Personal Data should never be written directly on an email, as this form of communication is not secure. It should be sent in a password protected file attachment and only if necessary.
c) Personal data should never be transferred outside of the European Economic Area.
d) Employees should only keep password protected copies of personal data on their own computers.
e) Always access and update the central copy of any data.

9. DATA ACCURACY

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

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. Data will be held in as few places as necessary (staff should not create any unnecessary additional data sets). Staff should take every opportunity to ensure data is updated (for instance, by confirming a customer's details when they call). Robert Walpole and Partners will make it easy for data subjects to update the information that is held about them. Data should be updated as inaccuracies are discovered.

10. SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by Robert Walpole and Partners are entitled to:

a) ask what information the company holds about them and why.
b) ask how to gain access to it.
c) be informed how to keep it up to date.
d) be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made in writing to a company partner. There might be a charge associated with such request to be advised at the time of enquiry. Robert Walpole and Partners will aim to provide the relevant data within 14 days. The identity of anyone making a subject access request will always be verified before handing over any information.

11. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Robert Walpole and Partners will consider disclosing requested data where appropriate exemptions apply under the current data protection regulations. However, the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

12. PERSONAL DATA BREACH

The Information Commissioner's Office's (ICO) website (www.ico.org.uk) broadly defines personal data breach as "a security incident that has affected the confidentiality, integrity or availability of personal data."

Personal data breaches can include:

- Data being accessed by unauthorised person.
- Data being altered by unauthorised person.
- Data being send to an incorrect recipient.
- Data being passed on without proper authorisation.
- Data being lost or stolen.

Each personal data breach will be investigated by one or both business partners in order to establish the likelihood and severity of the resulting risk to people's rights and freedoms. These can include emotional distress, and/or physical and material damage, for example: identity theft or fraud, financial loss, damage to reputation. If it is established that such risk is likely, then the ICO will be notified within 72 hours of Robert Walpole and Partners becoming aware of the personal data breach. The notification will include:

a) Description of the personal data breach (categories and number of individuals concerned, categories and number of personal data records concerned).
b) The name and contact details of the person responsible for handling the investigation (for follow up queries).
c) Description of the likely consequences of the personal data breach.
d) Description of actions taken or to be taken to address the personal data breach (including measures to mitigate the possible adverse effects).

Depending on the nature and severity of the personal data breach, data subjects involved may need to be notified as well without undue delay.

All personal data breaches (facts relating to the breach, its effects and the remedial action taken) will be recorded in order to comply with accountability principle of the current data protection regulations, regardless of whether or not they need to be reported to the ICO.