Privacy Policy

Privacy & Cookies Policy

DATA PROTECTION POLICY

Context and overview
Introduction
Wendi Mclean Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

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

Why this policy exists
This data protection policy ensures Wendi Mclean Ltd:

- Complies with General Data Protection Regulation (GDPR) 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 and those whose data it holds from the risk of a data breach
- **Data Protection Law**
- The General Data Protection Regulation (GDPR) describes how organisations – including Wendi Mclean Ltd must collect, handle and store personal information.
- These rules apply regardless of whether data is stored electronically, on paper or on other materials.
- To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
- The General Data Protection Regulation (GDPR) is underpinned by six important principles. These say that personal data must:
- Be processed lawfully, fairly and in a transparent manner
- Be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Be accurate and, where necessary, kept up to date

- 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
- Be processed in a manner that ensures appropriate security of the personal data

People, risks and responsibilities

Policy Scope

This policy applies to:

- Wendi Mclean Ltd Offices
- All Staff and Volunteers of Wendi Mc Ltd
- All contractors, suppliers and other people working on behalf of Wendi Mclean Ltd It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation (GDPR). This can include:
- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Company contacts

Special category data

Special category personal data, previously called 'sensitive data', includes any data that identifies the religion, politics, trade union membership, health, ethnicity or sexuality of a data subject. Processes that require the processing of special category data need an accompanying Data Protection Impact Assessment. Approval by the assessor is required before processing takes place. Extra care should be taken to protect special category data.

Data Protection risks

This policy helps to protect Wendi Mclean Ltd and its clients from some very real data security risks. Including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately
- **Breaches of contract.** For instance, a contract cannot be completed because necessary data was lost or corrupted
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data
- **Financial penalty.** For instance, a data breach results in a fine from the Information Commissioner's Office

Responsibilities

Everyone who works for or with Wendi Mclean Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Board of Trustees** is ultimately responsible for ensuring that Wendi Mclean Ltd meets its legal obligations
- The **Data Protection Officer, Wendi Mclean, Director,** is responsible for:
- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and related polices, in line with agreed schedule
- Arrange data protection training and advice for people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Wendi Mclean Ltd holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data
- Approving any data protection statements attached to communications such as emails and letters
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles
- Ensuring departing staff no longer have physical or online access to Wendi Mclean Ltd data assets

General Staff Guidelines

- **All employees must add** any new data sets to the asset register and complete a DPIA (Data Protection Impact Assessment) and data flow maps
- **All employees must** have Service Level Agreements (SLA's) between partners, and it must be clear who are the Data Controllers and/or Data Processors
- The only people able to access data covered by this policy should be those who **need it for their work**
- Data **must not be shared informally**. When access to confidential information is required, employees can request it from their line managers
- Wendi Mclean Ltd **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.
- In particular, **strong passwords must** be used, and they should never be shared
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally
- 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
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer.

When data is stored on paper, is must 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 for some reason:

- When not required, the paper or files must be kept **in a locked drawer or filing cabinet**
- Employees must make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer
- **Data printouts must be shredded** and disposed of securely when no longer required

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

- Data must be **protected by strong passwords** that are changed regularly and never shared between employees
- If data is **stored on removal media** (like a CD or DVD), theses must be kept locked away securely when not being used
- Data must only be stored on **designated drives and servers**, and must only be uploaded to **approved cloud computing services**
- Servers containing personal data must be **sited in a secure location**, away from general office space
- Data must be **backed up frequently**. Those backups must be tested regularly
- Data must **never be saved directly** to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data must be protected by **approved security software and a firewall**

Data use

Personal data is of no value to Wendi Mclean Ltd 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.

When working with personal data, employees must ensure **the screens of their computers are always locked** when left unattended

- Personal data **must not be shared informally**. In particular, if shared by email it must be password protected and sent via the RDP. The password must be given via another means (not via text from phone that receive emails) as this form of communication is not secure
- Personal data must **never be transferred outside of the European Economic Area**. There may be exceptions to this when for operational reasons it is necessary to use cloud hosts based outside the EEA: in these cases, the relevant process must be assessed by means of a Data Protection Impact Assessment. Approval by the assessor is required before the processing takes place
- Employees **must not save copies of personal data to their own computers or on desktops of any laptop or computer**. Always access and update the central copy of any data

Data accuracy

The law requires Wendi Mclean Ltd to take responsible 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 Wendi Mclean Ltd must 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 must not create any unnecessary additional data sets. If you wish to create a new data set containing personal data, you must first inform the data protection officer and create an entry in the Wendi Mclean Ltd Data Asset Register
- Staff must **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call
- Wendi Mclean Ltd will make it **easy for data subjects to update the information** Wendi Mclean Ltd holds about them. For instance, via the company website
- Data must be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it must be removed from the database

- If you are listed on the Data Asset Register as the owner of a data asset, it is your responsibility to ensure the asset is checked regularly as required.

Subject access requests

All individuals who are the subject of personal data held by Wendi Mclean Ltd are entitled to:

- Ask **what information** the company holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Be informed how the company is **meeting its General Data Protection Regulation (GDPR) 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 by email, addressed to the data protection officer at enquiries@wendimclean.com. The Company can supply a standard request form, although individuals do not have to use this.

The data protection officer will always verify the identity of anyone making a subject access request before handing over the information. Subject access requests must always be referred to the data protection officer.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation (GDPR) allows personal data to be disclosed to law enforcement agencies or other public authorities without the consent of the data subject

Under these circumstances, Wendi Mclean Ltd will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from the Company's legal advisers where necessary

Providing information

Wendi Mclean Ltd 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

To these ends, the company has a Privacy Policy, setting out how data relating to individuals is used by the company

This is available on request. A version of the policy is also available on the company's website

Actions in the event of a suspected data breach
Wendi Mclean Ltd has a Data Breach Plan. Should you suspect a data breach has occurred, refer to this plan and act to report the suspected breach. Examples of possible data breaches are:

- Emailing or posting personal data to an unintended recipient
- Accidental deletion of data that is still required for a process, with no back-up
- Loss or theft of a computer or device holding personal data, or of papers holding personal data
- A cyberattack on a work computer or device