



# DATA PROTECTION POLICY

22nd June 2020

This policy will be updated as our business changes in line with new legislation and statutory guidance. It will be reviewed and updated as necessary.



# Wolverhampton SFA – Data Protection Policy

## Introduction

Wolverhampton SFA needs to gather and use certain information about individuals.

These can include students, coaches, volunteers, and other people the organisation has a relationship with or may need to contact.

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

This data protection policy ensures Wolverhampton SFA:

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

## Data Protection Law

The Data Protection Act 2018 and the GDPR (which also forms part of UK law) describes how organisations, including Wolverhampton SFA, 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.

Article 5 of the GDPR sets out key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');



## Wolverhampton SFA – Data Protection Policy

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

### Policy Scope

This policy applies to:

- All staff and volunteers of Wolverhampton SFA
- All contractors, suppliers and other people working on behalf of Wolverhampton SFA

It applies to all data that the association holds relating to identifiable individuals, even if that information technically falls outside of the Act. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- (plus, any other relevant information relating to individuals)

### Data Protection Risks

This policy helps to protect Wolverhampton SFA from data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately
- **Failing to offer choice.** For instance, all individuals should be free to choose how the association uses data relating to them.
- **Reputational damage.** For instance, the association could suffer if an individual successfully gained access to sensitive data.

### Responsibilities

Everyone who works for or with Wolverhampton SFA has some responsibility for ensuring data is collected, stored and handled appropriately.

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

- The Officers are ultimately responsible for ensuring that Wolverhampton SFA meets its legal obligations.
- The Data Protection Officer (Gavin Hawkins – Association Secretary), is responsible for:
  - Keeping the Officers updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.



## Wolverhampton SFA – Data Protection Policy

- Dealing with requests from individuals to see the data Wolverhampton SFA holds about them (also called “subject access requests”).
- Checking and approving any contracts or agreements with third parties that may handle the association’s sensitive data.
- The Officers are responsible for:
  - Ensuring all systems, services and equipment used for storing data meet acceptable safety standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, the association is considering using to store or process data. For instance, cloud services.
  - Approving any data protection queries from journalists or media outlets such as newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

### General Staff Guidelines

- 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, staff can request it from their line managers.
- Wolverhampton SFA **will provide training** to all staff and volunteers to help them understand their responsibilities when handling data.
- Staff should keep all data secure, by taking sensible precautions and following the agreed guidelines.
- Strong **passwords must be used**, and they should never be shared.
- 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.
- Staff **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 should be directed to the data controller.

When 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.

- When not required, the paper or files should be **kept in a locked drawer or filing cabinet**.
- Staff should make sure paper and hard copies are **not left where unauthorised people could see them**, e.g. left on a printer.
- **Data printouts should 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.



## Wolverhampton SFA – Data Protection Policy

- Data should be **protected by strong passwords** that are changed regularly and never shared between staff.
- If data is **stored on removable media** (SD cards, etc.), these should be kept locked away when not being used.
- Data should only be stored on **designated drives and servers** and should only be uploaded to **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the association's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software**.

### Data Use

Personal data is of no use to Wolverhampton SFA unless the association can make use of it. However, it is when personal data is accessed and can be used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, staff should ensure **the screens of their computers are always left locked** when left unattended.
- Personal data **should not be shared informally**. It should never be sent by email, as this form of communication is not secure.
- Data must **be encrypted before being transferred electronically**. The data officer can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**
- Staff **should not save copies of personal data on their own computers**. Always access and update the central copy of any data.

Wolverhampton SFA's Privacy Policy provides specific guidance on the use, storage, retention and deletion of personal data.

### Data Accuracy

The law requires Wolverhampton SFA 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 Wolverhampton SFA should put into ensuring its accuracy.

It is the responsibility of all staff 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.



## Wolverhampton SFA – Data Protection Policy

- Wolverhampton SFA will make it **easy for data subjects to update the information** held on them, for instance, via the association website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

### Subject Access Requests

All individuals who are the subject of personal data held by Wolverhampton SFA are entitled to:

- Ask **what information** the association holds about them and why
- Ask **how to gain access** to it
- Ask for **information to be deleted**
- **Restrict** processing
- Be informed **how to keep it up to date**
- Be informed how the association is **meeting its Data Protection obligations**.

If an individual contacts the association requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by letter to Wolverhampton SFA and addressed to the Data Controller.

- A charge will not be requested in most circumstances
- Wolverhampton SFA will reply within 30 days

The Data Controller will always verify the identity of anyone making a subject access request before providing information.

### Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Wolverhampton SFA will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the Board and from the association's legal advisers where necessary.

### Providing Information

Wolverhampton SFA 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 association has a privacy statement and policy, setting out how data relating to individuals is used by the association. This is available on request.

# Wolverhampton SFA – Data Protection Policy



## Personal Data Breaches

*Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.