Policy Name	GDPR/Data Protection Policy
Last reviewed	September 2021
Next Review	September 2022
Reviewed By:	HR

DATA PROTECTION POLICY

INTRODUCTION

Active Fusion 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.[1]

This 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 General Data Protection Regulation (GDPR), which came into effect in May 2018.

This policy requires staff to ensure that the Data Controller be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Contents:

1. Overview
2. Scope and responsibilities
3. Data Protection law
4. GDPR Provisions
5. General Staff Guidelines
6. Data Storage
7. Data Use

Appendices:

8. Categories of personal data
9. Establishing a central data register

1. OVERVIEW:

1.1 Policy Statement

This Policy ensures the Company;

- 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 risks of a data breach.

This policy should be read in conjunction with the Homeworking and IT Policies. All the principles of data storage, processing, and disclosure of information apply equally to data used in the office, any other place of work or in the home.

1. SCOPE AND RESPONSIBILITIES

1.1 Employee responsibilities

This policy applies to all staff, volunteers and other people working on behalf of the Company. It applies to all data that the Company holds relating to identifiable individuals, for example a record of their name, address or telephone number. We are not permitted to handle or process such data without satisfying a relevant 'condition for processing'. These are set out in the GDPR and are **not optional**. You must be familiar with this policy and comply with its terms. We may supplement or amend this policy with additional guidelines from time to time.

As our Data Controller, Jonny Allan (Head of Operations) has overall responsibility for the day-to-day implementation of this policy. The Data Controller is also required to:

· Keep the director & trustees updated about data protection responsibilities, risks and issues

· Review all data protection procedures and policies on a regular basis (including relevant information security procedures in the IT Policy).

· Respond to individuals such as clients and employees who wish to know what data is being held on them by Active Fusion.

· Check and approve with third parties that handle the company's data any contracts or agreement regarding data processing.

1.2 GDPR Provisions

The GDPR **emphasises** the need for transparency in relation to the use of personal data by organisations. Organisations must provide 'fair processing' information to their customers and employees via a Privacy Notice. This information is extensive and includes items not currently mandatory under the 1998 Data Protection Act. Examples include:

• The legal basis for processing.

• The categories of personal data being processed.

• Details of any third party recipients.

• The intended retention period.

The definition of what information counts as 'personal data' is also being expanded. Firstly, online identifiers (such as IP addresses and cookies) will now be regarded as personal data. Secondly, there is a wider definition of 'special category' personal data – in other words sensitive data such as information relating to someone's *racial or ethnic origin, their political opinions, religious or philosophical beliefs, their sex life or sexual orientation*.

The GDPR significantly increases the rights of individuals and as a result, we may see an increase in requests from data subjects. We are obliged to respond to such requests within one month[2].

A summary of changes under the GDPR is given in the table below.

Summary of GDPR Changes

Data Subject Right	Changes under GDPR
The right of access	The GDPR **expands** the mandatory categories of information which must be supplied in connection with a data subject access request including information about a data subject's right to complain to the Data Protection Authority (DPA).
The right to erasure	The GDPR creates a **broader right** to erasure such as where the personal data is no longer needed for its original purpose or where the lawful basis for the personal data processing is the data subject's consent.
The right to restrict processing	Under the GDPR, there are a **much broader** range of circumstances in which data subjects can require that the processing of their personal data be restricted. Examples include the accuracy of the personal data being contested or the personal data is no longer needed for its original purpose.
The right to data portability	**A new right** under GDPR which provides data subjects the right to receive a copy of their personal data in a commonly used machine readable format, and have their personal data transferred from one data controller to another.
The right to object	The GDPR now puts the obligation on the Data Controller as it requires the Data Controller to cease processing unless it can demonstrate that it either has compelling grounds for continuing the processing, or

	that the processing is necessary in connection with its legal rights.
The right to rectification	As per the current EU Data Protection Directive, data subjects have the right to rectification where their personal data is shown to be incorrect.

1.3 Central data register

In preparation for the new legislation Active Fusion needs to establish a central data register. This register becomes our 'single source of truth' detailing the characteristics and processing activities for all personal data which our organisation is ultimately accountable for. The register must be regularly checked and updated to ensure its integrity over time. The data controller will build a data flow map based on the register contents to provide a visual representation of the various flows of personal data both internal and external to our organisation.

Any individual or business function with responsibility for processing data will need to gather information for the central register. A checklist tool and further guidance will be provided to staff for this purpose (see Appendix 2).

2. RISKS AND BREACH NOTIFICATION

2.1 Data protection risks

This policy helps to protect the Company from some very real 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 company uses data relating to them
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Failure to do so puts the company at risk of a heavy sanction. Fines have been increased under the GDPR.

2.2 Breach Notification

The GDPR defines a personal data breach as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

The Company would have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

In the event of a data breach, you must immediately contact the data controller who will investigate and take further action as appropriate.

3. SUBJECT ACCESS REQUESTS

3.1 Requests for information

All individuals who are the subject of personal data held by the Company 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 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 by email, addressed to the data controller at info@activefusion.org.uk The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

3.2 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 Active Fusion will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the director & trustees and the company's legal advisers where necessary.

4. TRAINING AND INFORMATION

4.1 Staff training

The company will provide training to all staff on data protection matters on induction and on a regular basis thereafter. Employees **should request help** from their line manager or speak to the Data Controller if they are unsure about any aspect of data protection.

The organisation will review and ensure compliance with this policy at regular intervals.

5. GENERAL STAFF GUIDELINES

5.1 Handling Data

- 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 data is required, employees can request it from their line managers.
- 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. Passwords must be regularly changed and access to company data should be confined to current employees.

- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Regular audits of data used should be undertaken to inform the central data register (as a minimum on an annual basis). The checklist provided in Appendix 2 can be used for this purpose.

5.2 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to your Line Manager.

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 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.

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

- Data should be protected **by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD or data stick) these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an approved cloud computing services e.g. Sharepoint, Dropbox for business.
- 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 Company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones
- Data should never be stored on home computers or laptops
- All servers and computers containing data should be protected by **approved security software and a firewall**.

5.3 Data use

Personal data is of no value to the Company 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 should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. ESP can explain how to send data to authorised external contacts.
- Personal data **should not be transferred out of the EEA**.
- Employees **should not save copies of personal data** to their own computers. Always access and update the central copy of any data.

5.4 Data accuracy

The law requires Yorkshire Sport Foundation to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that personal data is accurate, the greater the effort the Company 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.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer cannot be reached on their stored telephone number, it should be removed from the database.

Appendix 1

Personal Data

What is personal data?

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

Special Categories of Data (Sensitive Data) as defined in the General Data Protection Regulation (GDPR) includes:

• Racial or ethnic origin

• Political Opinions

• Religious or philosophical beliefs

• Trade union membership

• Data concerning health or sex life and sexual orientation

• Genetic data

• Biometric data where processed to uniquely identify a person

Appendix 2

Establishing a Central Data Register

Anyone with a responsibility for processing personal data must complete the following checklist to inform the central data register. These records can be requested and scrutinised by the Information Commissioners Office (ICO) and as such must be accurate and regularly updated.

What data is being collected?	
From whom is data collected?	
Why is the data being collected?	
How is the data being processed?	
What is the legal basis for each processing operation?	
Where is the data being stored?	
How long is the data retained?	
Who has access to the data?	
To where and to whom is the data being transferred?	

[1] A full list of business, personal and sensitive personal data we may process is provided in the Appendix.

[2] Unless they are manifestly unfounded, excessive or a National legislative measure has been introduced allowing the access to be refused.