

---

## DATA PROTECTION POLICY AND PROCEDURE

### 1.1. Policy

It is the policy of Active Lancashire to fully comply with the requirements of the Data Protection Act 2018 (which reference includes any replacement legislation) and to abide by its obligations in accordance with the Information Commissioner's office.

### 1.2. Aim

This document aims to outline the responsibilities of Active Lancashire as the data controller under the terms of the Data Protection Act. All staff have responsibility to process all personal data in line with this document and the Data Protection Act principles.

### 1.3. Scope

This policy and procedure is applicable to all staff of Active Lancashire and to those who in the course of their duties may be party to information held by Active Lancashire together with the data subjects themselves.

### 1.4. Introduction

This document outlines the steps which all members of Active Lancashire must take to ensure compliance with the Data Protection Act 2018 ("the Act").

The Act includes all Personal Data that is held automatically, including word-processed documents, databases and emails. It also extends to Personal Data held in manual records where these can be accessed by reference to a person.

All members of Active Lancashire have a duty to ensure compliance with the Act.

### 1.5. Definitions

Definitions under the Data Protection Act 2018 are as follows:

**"Data"** means any information which is stored in a form to which the Act applies including documents, images and sound.

**"Data Controller"** means the person or organisation which determines the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the Act. Active Lancashire is the data controller of all personal data used by the organisation for any of its purposes.

**"Data Processors"** means any person other than a staff member of the Data Controller who processes Data on behalf of the Data Controller. This would include people such as market researchers, consultants, contractors, suppliers and/or partner organisations who collect Personal Data on behalf of the Data Controller.

**“Data Subject”** means an identifiable or identified living individual who is the subject of the Personal Data held by Active Lancashire. A Data Subject could be anywhere in the world but must be living. All data subjects have legal rights in relation to their personal information.

**“Personal Data”** means Data which relates to a living individual who can be identified from that Data or from that Data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. Personal data can be factual (for example, a name, address or date of birth) or it can include any expression of opinion about that individual, their actions and behaviour and any indication of the Data Controller, its staff or any other person’s intentions towards that individual.

**“Processing”** means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, sharing, erasing or destroying it.

**“Relevant Filing System”** means any set of information relating to individuals which is not processed automatically but which is structured either by reference to individuals or criteria relating to individuals in such a way that specific information relating to a particular individual is readily accessible. This would include any paper files relating to individuals.

**“Sensitive Personal Data”** means Personal Data about an individual’s racial or ethnic origin, political opinions, religious or other similar beliefs, membership of a trade union (or non-membership), physical or mental health or condition, sex life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that individual, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

## 1.6. The eight Data Protection Principles

The Data Protection Act 2018 contains eight governing Principles relating to the collection, use and disclosure of data, and the rights of the subject to have access to Personal Data concerning themselves.

Anyone processing personal data must comply with the eight enforceable principles for good practice. These provide that personal data must be:

- Processed fairly and lawfully in line with individuals’ rights;
- Processed for limited purposes and in an appropriate way;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept longer than necessary for the purpose;
- Processed in line with data subjects’ rights;
- Secure against loss or misuse;
- Not transferred to people or organisations situated in countries without adequate

protection.

### 1.6.1. The First Principle

*Personal Data should be processed fairly and lawfully and, should not be processed unless certain conditions are met.*

All Personal Data processed must satisfy at least one of the conditions of Schedule 2 of the Act. Staff should not process Personal Data unless the requirements of Schedule 2 can be satisfied:

- With consent;
- To perform a contract with the individual;
- Under a legal obligation;
- To protect the vital interests of the individual;
- To carry out public functions conferred by or under enactment;
- For the administration of justice; and
- To pursue the legitimate interests of the data controller unless prejudicial to the interests of the individual.

Sensitive Personal Data processed must meet at least one of the conditions of Schedule 2 (above). In addition, it must also satisfy one of the conditions of Schedule 3 of the Act. Staff should not process Sensitive Personal Data unless the requirements of Schedule 3 can be satisfied:

- With explicit consent;
- Exercising or performing any right or legal obligation conferred or imposed on the data controller in the context of employment;
- To protect the vital interests of the individual where consent cannot be given or is unreasonably withheld;
- By certain non-profit bodies in the course of their legitimate activities;
- Where the information has manifestly been made public;
- In any legal proceedings;
- To carry out certain government functions (justice, government department, crown);
- For medical purposes undertaken by a Health Professional or suitably qualified individual; and
- Certain ethnic monitoring to ensure quality.

### 1.6.2. The Second Principle

*Personal Data will be obtained for only one or more specified lawful purposes and will not be further processed in any manner incompatible with that purpose or those purposes.*

Personal Data obtained for one stated purpose cannot be used for a completely different purpose without the individual being informed of the different purpose.

### **1.6.3. The Third Principle**

*Personal Data will be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed.*

Uniform information should not be held about all Data Subjects. Personal Data should only be kept if it is really necessary for a particular activity or operation.

### **1.6.4. The Fourth Principle**

*Personal Data shall be accurate and, where necessary, kept up to date.*

This obligation will apply to Personal Data not only obtained directly from the Data Subject but also to Personal Data obtained from third parties. Reasonable steps must be taken to ensure that any Personal Data which is obtained is accurate. Data Subjects may ask Active Lancashire to correct personal data relating to them which they consider to be inaccurate. Any requests for correction by a Data Subject will be dealt with by the Business Development Manager. If a member of staff receives such a request but does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Senior Leadership Team.

### **1.6.5. The Fifth Principle**

*Personal Data processed for any purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes.* Active Lancashire has retention periods in place for different categories of personal data.

### **1.6.6. The Sixth Principle**

*Personal Data will be processed in accordance with the rights of Data Subjects under this Act.* The rights of the Data Subject include the following:

- To request access to the information held about them, the purpose(s) for which the information is being used and those to whom it is or may be disclosed;
- To prevent processing likely to cause damage or distress;
- To prevent processing for the purposes of direct marketing;
- To be informed of the logic behind any automatic decision making;
- To take action for compensation if they suffer damage for any contravention of the Act by the Data Controller; and
- To take action to rectify, block, erase or destroy inaccurate data.

### **1.6.7. The Seventh Principle**

*Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of or damage to Personal Data.*

An adequate level of security must be in place for the handling of all Active Lancashire's Personal Data from collection through to disposal. This is all data held on computers (including email) and in manual filing systems (including both formal and informal notes and records). It also applies to Personal Data handled by external contractors, consultants and partners on behalf of Active Lancashire. When using these agencies, a written contract should be entered into which ensures that Active Lancashire's Data Protection Policy and Procedure is complied with at all times.

#### **1.6.8. The Eighth Principle**

*Personal Data must not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.*

There are exceptions to the general rule which may allow information to be transferred outside the EEA. These exceptions can be summarised as follows:

- With consent of the Data Subject;
- To make or perform a contract including between Active Lancashire and the Data Subject, or to protect the vital interests of the Data Subject;
- In legal proceedings for the establishment, exercise or defence of legal claims;
- To protect the vital interests of the Data Subject;
- For substantial public interest grounds;
- Where the information is on a public register; and/or
- On terms approved by the Information Commissioner or where authorised by the Information Commissioner.

Active Lancashire needs to be able to justify its reasons for transferring data if using the above criteria for transfers outside the EEA. Staff must seek authorisation from the Senior Leadership Team prior to transferring any Personal Data to any country or territory outside of the EEA.

#### **1.7. Procedure**

This document is intended to assist everyone within Active Lancashire to comply with the Act. Active Lancashire as a Data Controller will hold the minimum Personal Data necessary to enable it to perform its functions, and the data will be erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and up-to-date, and that inaccuracies are corrected without undue delay. Active Lancashire will provide to any individual who requests it, (in a manner specified by the Act) a formal reply to all enquiries made by that individual in accordance with the rights of Data Subjects.

It is the responsibility of every employee of Active Lancashire to ensure compliance with not only Active Lancashire's Data Protection Policy and Procedure but the Act itself. Active

Lancashire expects all of its employees to comply fully with this policy and procedure and the Act when processing Personal Data as part of their employment or research for Active Lancashire.

This document does not form part of any employee's contract of employment and may be amended at any time. Active Lancashire may supplement or amend this document by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Disciplinary action may be taken against any employee who breaches this policy and procedure or any other instructions relating to the Act or the Act itself.

#### **1.7.1. Responsibilities**

All employees have a general duty to observe the Act, any specific instructions given by Active Lancashire and any procedures relating to the Act. It is the responsibility of each employee to assist to maintain compliance with the Act in the relevant area. Employees should not disclose Personal Data that comes into their possession to other people unless this is necessary to perform their duties and in compliance with the Act.

#### **1.7.2. Exemptions**

A small number of activities are exempt from certain provisions of the Act. One such activity relevant to Active Lancashire is using Personal Data for research purposes, which is exempt from a limited number of principles of the Act. However, the results of the research should not identify the Data Subject.

Other exemptions that are available are of a very specific nature. They relate to matters such as National Security, Crime and Taxation and Health matters. These exemptions that in certain cases allow Active Lancashire to disclose data without consent are dealt with in the section of this Code of Practice that relates to the disclosure of Personal Data.

The guidelines issued by the office of the Information Commissioner set out all exemptions from the Act. These can be viewed on the Information Commissioner's website at: [www.ico.gov.uk](http://www.ico.gov.uk)

#### **1.7.3. Access to Personal Data**

Access to Personal Data includes disclosures and Subject Access Requests.

Disclosure of Personal Data is permitted under the 2018 Act where Active Lancashire has both notified the usage to the Information Commissioner and complied with the requirements of both Principles 1 and 2 of the Act. It is essential that at the time the data is collected, Data Subjects are informed of the purposes for which it will be used and the individuals or organisations to whom it may be disclosed. If it is proposed to use the information obtained for direct marketing purposes, Data Subjects should be informed of this purpose at this time and given the opportunity to decline this usage of the data.

Within the terms of the Act, the following are authorised persons to whom Personal Data may be disclosed:

- The Data Subject, or someone acting on behalf of the Data Subject who has been nominated in writing and notified to Active Lancashire.

Within the terms of the Act Personal Data may only be disclosed where the purposes have been notified to the Information Commissioner and where the Data Subject's informed consent has been obtained. When data is used for the purpose of direct marketing care must be taken to ensure that the Data Subject has not objected to this processing either at the date of collection or at a later date.

Within the terms of the Act the following are purposes where data may be disclosed to third parties without the consent of the Data Subject:

- For legal purposes, if the Personal Data is required by statute, rule of law or Court Order; is required to obtain legal advice; or required for legal proceedings in which the person making the disclosure is a party or witness;
- To safeguard national security based on a certified request from a Cabinet Minister, Attorney General or Lord Advocate;
- For the prevention of crime and for taxation purposes. Disclosures for these reasons will only occur if Active Lancashire is satisfied as to the purpose of such a request and the likelihood of substantial prejudice if the request was refused;
- To protect the vital interests of the Data Subject; and
- To carry out regulatory functions such as securing the health, safety and welfare of persons at work.

It should be remembered that requests for disclosure for the purposes listed above should be considered on a case by case basis only by the Business Development Manager.

#### **1.7.4. Responding to disclosure requests**

All requests for disclosure of Personal Data from persons outside Active Lancashire must be treated with caution by all staff. To ensure against disclosure to unauthorised persons and/or for unauthorised purposes within their relevant area staff should take account of the following guidelines:

- Personal Data must not be disclosed to an external body over the telephone. Individuals making such enquiries should be asked to confirm in writing why the information is required and be informed of Active Lancashire's requirement to comply with the Act. Wherever possible (except where an exemption applies) the Data Subject should be informed of the enquiry to enable them to respond directly.
- Parents, relatives and guardians should be informed of Active Lancashire's requirement to comply with the Act if making representation on behalf of a child or young person.
- All requests from outside agencies such as the Police, DSS, Inland Revenue, Local

Authorities Overseas Embassies or High Commissions should be submitted in writing and forwarded to the Business Development Manager.

#### **1.7.5. Subject rights**

The Act gives certain rights to individuals in respect of Personal Data held about them. These rights are:

- the right of Subject Access;
- the right to prevent processing likely to cause damage or distress;
- the right to prevent processing for the purposes of direct marketing;
- the right to be informed of the logic behind any automatic decision making;
- the right to take action for compensation if they suffer damage by any contravention of the Act by the Data Controller;
- the right to take action to rectify, block, erase or destroy inaccurate data; and
- the right to ask the Commissioner to assess whether or not it is likely that any processing of Personal Data has not been carried out in accordance with the Act.

The following are the procedures that must be followed if an individual requests Active Lancashire to comply with these requirements of the Act.

##### **1.7.5.1. Subject Access Requests**

Data Subjects have the right to be informed whether Personal Data about them is being processed by Active Lancashire and the right to receive a copy of that Personal Data together with details of the purpose for which it is being processed and to whom the data might be disclosed within 30 days of making that request. This entitlement relates to all Personal Data held about an individual, whether in computerised records or in a structured manual file.

A Subject Access Request must be in writing which includes email, but does not have to specifically refer to Subject Access, Data Protection or the Act. An individual could ask for all information that Active Lancashire holds about them.

All requests for Subject Access must be immediately passed to the Business Development Manager.

After an acknowledgement letter is sent to the applicant, the Designated Officer will forward a copy of the request to the relevant Senior Leadership Team area requiring the retrieval of the data by a specific date. The results of the retrieval must be returned to the Designated Officer in a sealed envelope, marked "Strictly in Confidence", by the specified date. "Nil" returns are also required.

The Business Development Manager will co-ordinate the formal reply to the applicant, or will advise them that no Personal Data relating to them is held.

#### **1.7.5.2. Responding to Subject Access Requests**

Certain rules must be followed by the data user when retrieving Personal Data in response to a Subject Access Request. These are that:

- The data need not necessarily be provided as a print-out. The Data Controller may choose to write or type the data to be supplied, with any accompanying explanation;
- The data must be intelligible to the Data Subject;
- Having received a request, no special amendments or deletions of data can be made which would not otherwise have been made;
- If Personal Data includes information which identifies another individual, (and was not originally provided by the Data Subject) the consent of the third party should be sought before the disclosure is made. If the third party does not consent to this disclosure the information may be edited out of the reply to the Data Subject providing the third party remains unidentifiable. Third party data should not be edited out completely - for example, X and Y could be used instead of full names;
- There may be limited circumstances where it may be reasonable in all the circumstances to comply with the request without the consent of the other individual. However, to determine if this is the case assistance from the Senior Leadership Team should be sought;
- If data retrieved is used to make an automatic decision which may significantly affect the Data Subject, an explanation must be provided of the logic underlying the decision making process.

#### **1.7.6. Prevention of processing**

A Data Subject is entitled to request that Active Lancashire either ceases or does not begin to process information that the Data Subject considers may cause unwarranted substantial damage or distress to them or another. These requests must be received in writing from the individual and should be forwarded to the Designated Officer.

After an acknowledgement letter is sent to the applicant, the Designated Officer will forward a copy of the request, if necessary, to the relevant Senior Leadership Team member requiring that they consider the application and make a decision whether or not to continue processing based on all the relevant circumstances of the case. The Designated Officer will, within 21 days of the original request being received, send a written reply to the individual setting out the Senior Leadership Team member decision to either comply with the request, or to explain the reasons why Active Lancashire feels that the request is unjustified. If the decision taken is to cease processing the data, the relevant Senior Leadership Team member will immediately take steps to comply with this action.

#### **1.7.7. Information security**

Under the Data Protection Act, security measures apply not only to the security of computer hardware and storage media but also to source documents including manual records, printouts and oral disclosure. Security measures are also applicable throughout the use and processing of Personal Data, including the handling, transmission, disclosure and disposal of documents containing Personal Data.

Active Lancashire takes appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This includes procedures such as the internet usage policy and email policy and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Staff must take reasonable steps to keep personal data secure against loss or misuse.

Where external organisations are used to process Personal Data on Active Lancashire's behalf additional security arrangements needs to be implemented in written contracts with those organisations to safeguard the security of personal data. Staff should consult the Senior Leadership Team to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement. Active Lancashire's procedure outlined in this document has incorporated security measures.

The Senior Leadership Team is responsible for reviewing from time to time that adequate security arrangements for Personal Data are in place. Although this responsibility may be delegated, it is incumbent on the Senior Leadership Team to ensure such reviews are conducted as necessary and that staff are aware of their responsibilities with regard to Data Protection.

#### **1.7.8. Data protection and email**

Personal Data includes any personal information stored in email messages and, potentially, email addresses themselves. Staff must therefore comply with this policy and procedure in relation to any Personal Data which is sent, received or stored in the form of an email.

#### **1.7.9. Data protection and the internet**

The provisions of the Data Protection Act apply equally to processing on the internet as they do to processing on all other information systems. When Personal Data is submitted to Active Lancashire via the website the following information must be supplied to the Data Subject:

- The purpose for which the data is collected;
- The description of the organisations or individuals to whom the data might be disclosed;
- Whether the Data Subject gives specific, informed and unambiguous consent for any direct marketing; and
- the right of the Data Subject to withdraw his consent to direct marketing at any time.

Where Active Lancashire receives Personal Data from another organisation, the relevant Senior Leadership Team member must ensure that the subsequent use of the Personal Data conforms to the information provided to the Data Subject. If any further subsequent use of this data is proposed that was not disclosed at the time of collection consent must be obtained from the Data Subject before commencing this processing.

Further guidance on Data Protection issues is available from the following websites:

- The office of the Information Commissioner at: [www.ico.gov.uk](http://www.ico.gov.uk); and
- The JISC Code of Practice for HE and FE Sectors at: [www.jisc.ac.uk](http://www.jisc.ac.uk).

### 1.8. Guidelines for Retention of Personal Data held by the Training Centre

Note: This is not an exhaustive list. For more information on data retention, please refer to Active Lancashire's Data Retention Policy.

Type of Data	Data Retention Period	Justification
<b>Learner Data</b>	During and up to 6 years from the end of the training course.	Contractual obligation to retain document.
<b>Learner Data funded through European Social Investment Fund Projects (e.g. Business Health Matters).</b>	10 years following the final payment by the Department for Work and Pensions	Required as evidence of compliance with ESF Funding Agreement.
<b>Personal data relating to participants of publicly funded projects</b>	During the project and up to 6 years from the end of the project.	Contractual obligation to retain documents  (2 years from 31 December following submission of accounts of completed project)

