DATA PROTECTION POLICY

Author: Vicky Knappett
Date: January 2018
Version: Draft

Addysg Oedolion Cymru
Adult Learning Wales

DATA PROTECTION POLICY

Status:		Draft
Equality impact assessment date:		27th Feb 18
Sent to SMT:		27th Feb 18
Sent to JNC:		12th March 18
Consulted on with staff:		
Implemented:		
Author:		Vicky Knappett
Due for Review:		

THIS POLICY IS ALSO AVAILABLE IN WELSH.

1.0 INTRODUCTION

1.1 Addysg Oedolion Cymru | Adult Learning Wales (referred to hereafter as AOC | ALW) needs to gather and use certain information about individuals (referred to hereafter as 'data subjects' in the course of its work. These individuals include learners; employees; partners; members; council members; and any other people that the organisation has a relationship with, or may need to contact. This policy describes how this personal data is collected, handled and stored to meet the organisation's obligations to data protection legislation and our commitment to the lawful and correct treatment of personal and sensitive information.

2.0 PURPOSE

2.1 This data protection policy sets out how AOC | ALW:

- complies with data protection law
- follows good practice
- protects the rights of individuals
- is transparent about how it stores and processes the data of individuals
- protects itself from the risk of a data breach
- has processes to follow in the event of a data breach
- has processes to follow in the event of a subject access request
- ensures that adequate processes and procedures are put in place to fulfil its obligations under the legislation
- ensures that staff who process data are adequately trained in data protection
- ensures that the organisation has an appropriate legal basis for its data processing activities

3.0 APPLICABLE LAW

3.1 The key pieces of legislation that inform this policy are:

- Data Protection Act **(DPA)**1998
- General Data Protection Regulation **(GDPR)** (effective 25/05/18)

4.0 SCOPE

4.1 This policy applies to all employees, volunteers, contractors, suppliers, members and other people working on behalf of AOC | ALW.

5.0 DEFINITIONS

5.1 Data breach: A data breach means a breach of security leading to the loss, destruction, alteration, unauthorised disclosure of, or access to, personal data.

5.2 Data Controller: The entity responsible for what personal information the organisation will hold and how it will be held or used. In this instance, the Addysg Oedolion Cymru | Adult Learning Wales is the data controller.
5.3 Data Subject: The individual whose personal information is being held or processed by the organisation, for instance: learners, potential employees, volunteers, employees and members.
5.4 Data Processor: The data processor is responsible for processing personal data on behalf of a controller.
5.5 Data Protection Officer: Person responsible for informing and advising the organisation and its employees about data protection obligations; monitoring compliance; and the first point of contact for the ICO and data subjects.
5.6 ICO: The UK's independent supervisory authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
5.7 Lawful Basis for Processing: The lawful bases for processing are set out in the GDPR. At least one of these must apply when the organisation processes data.
5.8 Personal Data/Information: information that relates to an identifiable living person who can be directly or indirectly identified.
5.9 Sensitive Data/Information: This includes race or ethnic origin; political opinions; religion or belief; trade union membership; physical or mental health; sex life and sexual orientation; criminal record; criminal proceedings in relation to a data subject's offences
5.10 Subject Access Request: a request for personal data from a data subject under the Data Protection Act 1998.
5.11 Supervisory Authority: Authority provided by each member state to monitor the application of the GDPR.

6.0 RESPONSIBILITIES

6.1 Every employee, volunteer, member, supplier and contractor of AOC | ALW has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and with data protection principles.

6.2 However, these people have key areas of responsibility:

6.3 SMT is defined as the 'Data Controller' and has ultimate responsibility for ensuring that AOC | ALW meets its legal obligations in respect of data protection.

6.4 The **Data Protection Officer** is currently the Senior Officer HR and is responsible for:

- Keeping SMT and Council 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
- Responding to queries and providing advice and guidance from employees and other individuals
- Responding to subject access requests
- Responding to data breaches
- Checking and approving any contracts or agreements with third parties who may handle AOC | ALW data

6.5 GDPR Working group is responsible for:

- Supporting the Data Protection Officer in the above tasks

6.6 The MIS and IT Manager is responsible for:

- ensuring systems, services and equipment used for storing data meet acceptable security standards
- performing regular checks and scans to ensure security hardware and software is functioning properly
- evaluating any third-party services that AOC | ALW is considering using to store or process data

6.7 The Senior Officer for Marketing and Communications is responsible for:

- approving any data protection statements attached to communications such as emails or letters
- communicating any data protection related queries from journalists or media outlets to the Data Protection Officer
- working with other staff to ensure that marketing initiatives abide by data protection principles

6.8 All staff are responsible for:

- ensuring that the only people able to access data covered by this policy should be those who need it for their work
- ensuring that data is not shared informally. When access to confidential information is required, employees can request it from their line managers
- attending training in relation to data protection when requested to do so
- keeping data secure by taking sensible precautions and following the guidelines below
- ensuring that they use strong passwords and never sharing their passwords
- personal data should not be disclosed to unauthorised people either within AOC | ALW or externally
- data should be regularly reviewed and updated and if no longer required, disposed of in accordance with the AOC |ALW Retention of Records Policy

- employees must seek advice and guidance from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection
- reporting data breaches **immediately** to the Data Protection Officer
- reporting any subject access requests promptly to the Data Protection Officer

7.0 DATA PROTECTION PRINCIPLES

7.1 The following principles underpin the applicable law relevant to this policy.

7.2 Data should be processed fairly, lawfully and transparently

7.3 This means that the organisation must:

- have legitimate grounds for collecting and processing the data it handles
- not use the data in ways that have unjustified adverse effects on data subjects
- be transparent about how it intends to use the data, and give data subjects fair processing notices when collecting personal data
- handle personal data in a manner that data subjects would reasonably expect
- not do anything unlawful with the data

7.4 Data should be obtained only for one or more of the purposes specified in the Data Protection Act and shall not be processed in any way which is incompatible with those purposes.

7.5 This means that the organisation must:

- be clear at the outset as to why we are collecting data and what we intend to do with it
- comply with fair processing requirements including the duty to give fair processing notices to data subjects when collecting their personal data
- comply with what the law says about notifying the ICO

7.6 Data processing shall be adequate, relevant and not excessive.

7.7 This means that the organisation must:

- hold data that is sufficient for the purpose of holding it for in relation to that data subject
- not hold more personal data than needed for that purpose

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

7.9 This means that the organisation must:

- take reasonable steps to ensure that any personal data it obtains is accurate

- ensure that the source of any personal data is clear
- carefully consider any challenges to the accuracy of that information
- consider whether it is necessary to update the information

7.10 Data should not be kept for any longer than is necessary

7.11 This means that the organisation must:

- review the length of time it keeps personal data
- consider the purpose or purposes it holds the information for in deciding whether and for how long to retain it
- securely delete data that is no longer required
- , archive or securely delete information if it goes out of date

7.12 Data should be processed in accordance with the rights of data subjects under the Act.

7.13 This means that the data subject has:

- a right of access to a copy of the information comprised in their personal data
- a right to object to processing that is likely to cause or is causing damage or distress
- a right to prevent processing for direct marketing
- a right to object to decisions being taken by automated means
- a right to have inaccurate data rectified in certain circumstances
- a right to claim compensation for damages caused by breach of the act

7.14 Data shall be kept secure by the Data Controller and any Processor.

7.15 This means that the organisation, and those organisations who process any data subject's information through contracted agreement with the organisation must:

- design and organise security to fit the nature of the personal data it holds and the harm that may result from an information security breach
- be clear about who in the organisation is responsible for ensuring information security
- make sure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well trained staff
- be ready to respond to any breach of security swiftly and effectively

8.0 LAWFUL BASIS FOR PROCESSING

8.1 At least one lawful basis for processing information must be identified and documented in accordance with the GDPR. The six lawful bases for processing are:

- **Consent** – the data subject has given clear consent for you to process their personal data for a specific purpose
- **Contract** – the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
- **Legal obligation** – the processing is necessary for you to comply with the law
- **Vital Interests** – the processing is necessary to protect someone's life
- **Public task** – the processing is necessary to perform a task in the public interest or for official functions and the task or function has a clear basis in law

8.2 The principle of accountability require AOC | ALW to demonstrate compliance with the GDPR and we are required to show which lawful basis we have applied to each processing purpose and can justify our decision.

8.3 The organisation has a record of the data it processes and the legal basis for processing it. This information is held with the Data Protection Officer.

9.0 DATA COLLECTION AND CONSENT

9.1 The GDPR sets high standards for consent which means offering individuals real choice and control over how organisations use their data. Consent should be obvious and require positive action to 'opt in'.

9.2 The organisation will ensure that data is collected within the boundaries defined in this policy whether the data is collected face to face; by telephone; by completion of forms such as application forms or enrolment forms; or electronically.

9.3 When collecting data, the organisation will ensure, wherever possible, that there is a fair processing notice in place and that the data subject:

- Is aware of the legal basis the organisation has for processing the data
- clearly understands why the information is needed
- understands what the information will be used for and what the consequences are should the individual decide not to give consent to processing
- understands who the data will be shared with and why
- has the option to consent to sharing the data
- grants explicit written or verbal consent to collect and share sensitive data wherever possible
- gives explicit consent to contact via email **agree**
- is competent enough to give consent and has given so freely without any **duress !**

9.4 The organisation will ensure that:

- it is clear, concise and specific about what processing it requires consent for and the purpose of the data collection
- it names any third party controllers who will rely on the consent
- it will make it easy for data subjects to withdraw the consent and it will tell them how to do so
- it will keep evidence of consent – who, when, how and what we told data subjects
- it will keep consent under review and refresh it if anything changes
- it will act on withdrawals of consent as soon as it can

9.5 These steps will ensure that the data subject has enough information for them to give informed consent to the organisation.

10.0 DATA STORAGE

10.1 All information and records relating to data subjects will be stored securely and will only be accessible to authorised staff and volunteers
10.2 Information will be stored for only as long as it is needed or required and will be disposed of appropriately in line with the Records, Retention and Destruction Policy.

10.3 When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it.

- when no longer required the paper or files will be kept in a locked drawer or filing cabinet.
- employees will make sure paper and printouts are not left where unauthorised people can see them, like on a printer or an unattended desk
- data printouts will be shredded and disposed of securely when no longer required.

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

- data will be protected by strong passwords that are changed regularly and never shared between employees
- if data is stored on removable media these should be stored securely and locked away when not in use
- data will be stored on designated drives and servers and should only be uploaded to an approved cloud computing service
- servers containing personal information will be sited in a secure location away from general office space
- data will be backed up frequently and backups will be tested regularly
- data will never be saved directly to laptops and other mobile devices like tablets or phones

- all servers and computers containing data will be protected by approved security software and a firewall.

11.0 DATA USE

11.1 Data use can be the greatest risk of loss, corruption or theft and these guidelines must be adhered to when using data:

- when working with personal data, employees should ensure the screens of their computers are locked when they are left unattended.
- data must be encrypted before being transferred electronically
- personal data should never be transferred outside of the European Economic Area
- employees should not save copies of personal data to their personal computers or drives and should always access the central copy of any data

12.0 DATA ACCURACY

12.1 The law requires AOW | ALW to take reasonable steps to ensure that data is kept accurate and up to date. It is the responsibility of employees working with personal data to take reasonable steps to ensure it is kept as accurately and as up to date as possible. These steps are as follows:

- data will be held in as few places as necessary, employees should not create any unnecessary data sets
- employees should take every opportunity to ensure that data is updated, for instance, by confirming a learners' details if they call.
- AOC | ALW will make it easy for data subjects to update the information that AOC | ALW holds about them
- data should be updated as inaccuracies are discovered. For instance, if a learner can no longer be reached on their stored phone number, it should be removed from the system
- AOC | ALW will ensure that everyone who processes personal information is appropriately trained to do so
- Everyone who processes personal information will be trained to report a suspected or actual breach of data management using the data protection breach reporting procedure (appendix 1)
- It is the Senior Officer for Marketing's responsibility to ensure that marketing databases are checked against industry suppression files every 6 months

13.0 DATA BREACHES

13.1 Under the GDPR all organisations have a duty to report certain types of data breaches to the ICO and in some cases, to the data subjects affected.

13.2 AOC | ALW will notify the ICO if a breach is likely to result in a risk to the freedom and rights of individuals. If unaddressed, such a breach is likely to have a significant detrimental impact on individuals, for example, resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

13.3 AOC | ALW will notify data subjects directly if the breach is likely to result in a high risk to the rights and freedoms of individuals. The threshold for notifying individuals is higher than for notifying the ICO.

13.4 ALL data breaches should be reported to the Data Protection Officer who will assess the impact of the data breach on a case by case basis.

13.5 A notifiable breach will be reported to the ICO within 72 hours of AOC | ALW becoming aware of the breach. (Failure to notify a breach when required to do so can result in a significant fine of up 10 million euros or 2% of our turnover.)

13.6 We will provide the following information to the ICO in the event of a high impact data breach:

- The nature of the personal data breach including the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned
- The name and contact details of the Data Protection Officer
- A description of the potential consequences of the data breach
- A description of the measures taken to deal with the data breach and measures taken to mitigate any possible adverse effects.

14.0 DATA SHARING

14.1 The organisation may share data with other agencies such as the local authority; funding bodies; and other voluntary agencies where it improves and promotes opportunities for adult learning and raises the profile of adult learning. This may require consent from data subjects if there is not a lawful basis to share the data.

14.2 Data subjects will be made aware in most circumstances, how and with whom their information will be shared through the use of clear fair processing notices located on the website; application forms; and other relevant documentation.

14.3 There are certain circumstances where the law allows the organisation to disclose data and sensitive data without the consent of the data subject. These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a data subject or another person
- If the data subject has already made the information public
- When conducting any legal proceedings, obtaining legal advice or defending any legal rights

- If anonymised, collecting data for equality and diversity purposes

15.0 SUBJECT ACCESS REQUESTS

15.1 All individuals who are subject of personal data held by AOC | ALW are entitled to:

- Ask what information the organisation holds on them and why
- Ask how to gain access to that information
- Be informed on how to keep it up to date
- Be informed how the organisation is meeting its data protection obligations

15.2 If in individual contacts the organisation requesting this information, this is called a subject access request.

15.3 Where possible, Subject Access Requests should be made directly to the Data Protection Officer at DPO@adultlearning.wales or to 7 Coopers Yard, Curran Road, Cardiff, CF10 5NB.

15. 4 AOC | ALW are committed to responding to Subject Access Requests within one month in line with the General Data Protection Regulations, but will extend the period by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

15.5 In every case, we will verify the identity of the person making the request.

16.0 THE RIGHT OF ERASURE

16.1 In addition to enabling individuals to access their personal information, the GDPR gives data subjects additional rights to erasure in certain circumstances. The right of erasure will apply when:

- Personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the data subject withdraws consent
- The data subject objects to the processing and there is no overriding legitimate interest for continuing the processing
- If the data has been unlawfully processed in breach of the Data Protection Act 1998 and GDPR
- If the data has to be erased to in order to comply with a legal obligation

17.0 FAIR PROCESSING NOTICES

17.1 Data subjects have the right to be informed about how we process their data. The GDPR sets out what information should be provided to data subjects and that the information supplied should be:

- concise, transparent, intelligible and easily accessible
- written in clear and plain language
- free of charge

17.2 In all cases, individuals will be informed of:

- the identity and contact details of the data controller's representative
- the purpose of the processing and the lawful basis for processing
- the legitimate interests of the controller or third party, where applicable
- any recipient or categories of recipients of the personal data
- retention period or criteria used to determine the retention period
- the existence of each data subject's rights
- the right to withdraw consent at any time, where relevant
- the right to lodge a complaint with the ICO
- the existence of automated decision making, and information about how decisions are made, and the significance of the consequences

18.0 THIRD PARTY CONTRACTORS

18.1 AOC | ALW has written agreements with third party organisations that process information. AOC | ALW are liable for third party compliance with the GDPR and we will only appoint processors who can provide "sufficient guarantees" that the requirements of the GDPR will be met and the rights of data subjects protected.

18.2 Contracts will contain the following written terms:

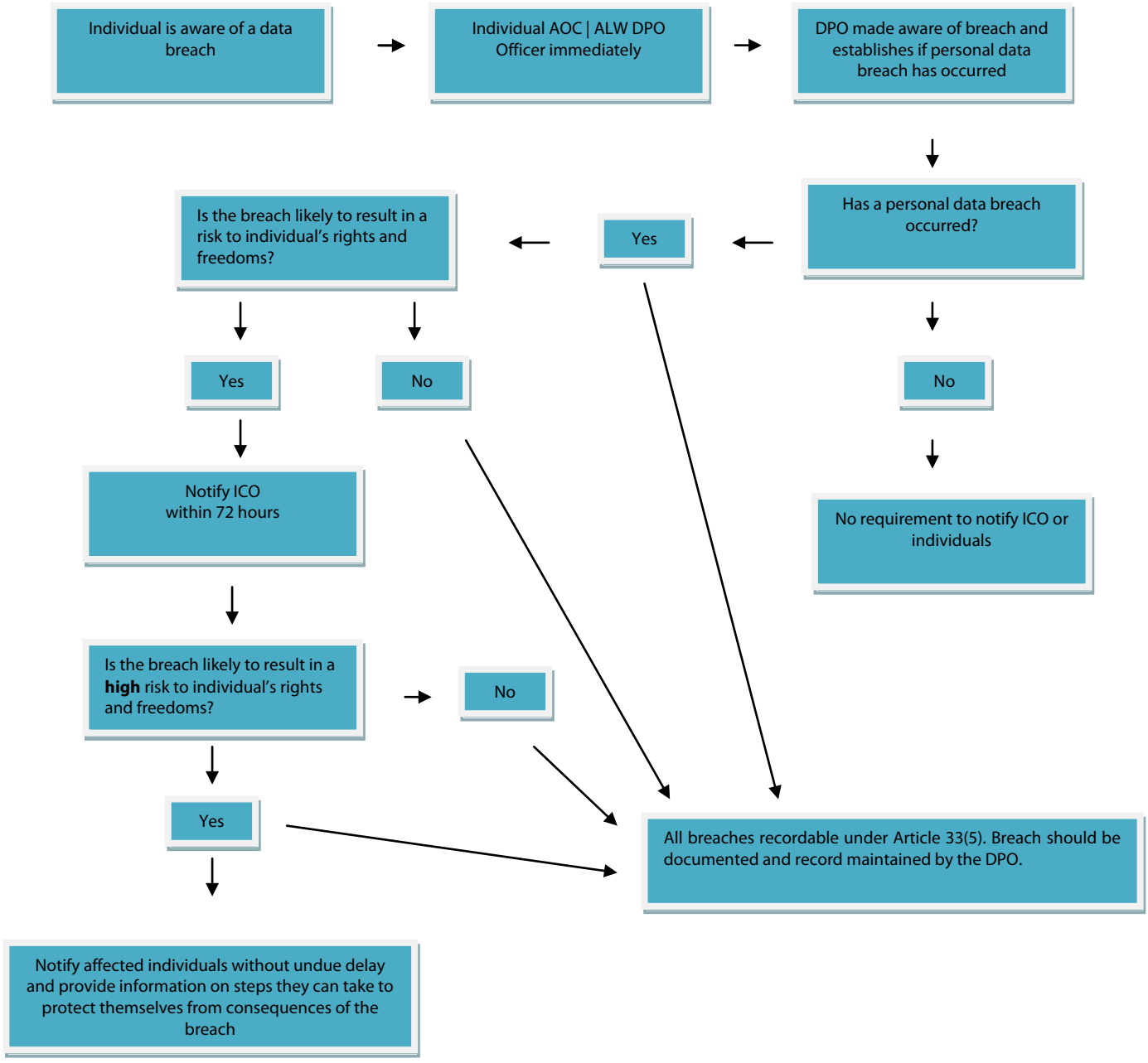
- The processor must only act on the written instructions of the processor
- The processor must ensure that people processing the data are subject to a duty of confidence
- The processor must take appropriate measures to ensure the security of the processing
- The processor must only engage a sub processor with the written consent of the controller
- The processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- The processer must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- The processor must delete or return all personal data to the controller as requested at the end of the contract

19.0 NON COMPLIANCE WITH THIS POLICY

19.1 There may be serious reputational and financial consequences for the organisation for non compliance with the Data Protection Act 1998 and the General Data Protection Regulations, if a complaint is made against the organisation to the ICO, or a data subject claims for compensation as a result of negligence.

19.2 Disciplinary action may be taken in line with the AOC | ALW disciplinary policy if members of staff do not adhere to the principles and guidelines laid out in this policy.

DATA PROTECTION BREACH REPORTING PROCEDURE



Appendix 2

EQUALITY IMPACT ASSESSMENT FORM

Policy, procedure, practice or form: Data Protection Policy	**Date of assessment:** 27th February 2018
1. Is this a new or existing policy, procedure, practice or form being assessed? This is a revised policy.	
2. Give a brief description of the policy, procedure, practice or form being assessed. The policy outlines the organisation's commitment to keeping data safe and the processes by which data subject access requests can be made, and security breaches dealt with.	
3. Please list any documents/evidence that have been used to inform this Equality Impact Assessment (e.g. demographic data; research findings; policies in similar institutions; survey data; equality monitoring data) Guide to the General Data Protection Legislation (ICO), 2017 GDPR, Filling in some of the detail (Hugh James presentation), 2017 Keeping Data Secure, What Happens when it all goes wrong (Hugh James presentation), 2017 Countdown to GDPR, (Eversheds), 2017	
4. Has any consultation, involvement or research with protected characteristic groups informed this assessment? (e.g. legal advice, staff consultation, stakeholder forums) Consultation will take place with the organisation's recognised union and the	

wider staff group.

5. Which protected characteristic groups will be positively or negatively affected by this policy, procedure, practice or form?

	Positively	Negatively	No impact	Not known
Race, including ethnic or national origin, colour or nationality	√			
Sex	√			
Gender identity	√			
Religion or Belief	√			
People with a disability	√			
Age	√			
Sexual orientation	√			
Marriage or civil partnership	√			
Pregnancy or maternity	√			

6. How will use of the Welsh language be positively or negatively affected by this policy, procedure, practice or form?

	Positively	Negatively	No impact	Not known
Opportunities to use the Welsh language			√	
Treating the Welsh language			√	

no less favourably than the English language.				

7. Can this policy, procedure, practice or form be revised to:

	Opportunities to use the Welsh language	**Treating the Welsh language no less favourably than the English language.**
Increase positive effects on:		
Decrease adverse effects on:		

8. How will the policy, procedure, practice or form impact on Addysg Oedolion Cymru/Adult Learning Wales' ability to comply with the Public Sector Equality Duty in Wales 2014 to eliminate unlawful discrimination, promote equality and foster good relations?

This policy has a positive impact on the safe keeping of sensitive personal data including protected characteristics in line with the relevant legislation.

9. Where no impact has been identified give reasons

10. List any positive impacts that have been identified

As in 8, protected characteristic data is afforded protection in line with the legislation surrounding 'special category' data.

11. List any negative impacts that have been identified

12. What action is required to overcome any identified negative impacts?

Impact / Issue	Action	How will this address the negative impact?	Who is responsible	Date for Completion

13. How will the policy, procedure, practice or form be monitored?

We will monitor the amount subject access requests and we will review the policy every 3 years in line with our policy timetable.

Prepared by: Vicky Knappett

Date 27-02-18

Approved by:

Date of next review: When policy is reviewed