Adam Price MS

DATA PROTECTION POLICY

**Scope**

* 1. This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers.
	2. All staff must be familiar with this policy and comply with its terms.
	3. Compliance with this policy is mandatory. Staff must also comply with any related policies and privacy notices. Any breach of this Data Protection Policy may result in disciplinary action
	4. The MS may supplement or amend this policy by additional policies and guidelines from time to time.
1. Introduction
	1. **Adam Price MS** (the “MS”) holds personal data about job applicants, employees, workers, constituents, suppliers and other individuals for a variety of purposes. For the purposes of this policy, and the privacy notices used by the MS, personal information has the same meaning as personal data.
	2. The MS recognises that the correct and lawful treatment of personal information will maintain confidence in them and will provide for the successful undertaking of their functions as an MS. Protecting the confidentiality and integrity of personal information is a critical responsibility that the MS takes seriously at all times.
	3. This policy sets out how the MS seeks to protect personal information and ensure staff understand the rules governing their use of personal information to which they have access in the course of their work.
	4. This policy applies to all personal information the MS processes regardless of the media on which that information is stored or whether it relates to past or present employees, workers, constituents, suppliers or any other individuals.
	5. For the purpose of this policy, the person responsible for data protection Adam Price MS, is:

Name: **Osian Evans**

Email address: **Osian.Evans@Senedd.Wales**

Postal address: 37 Wind Street, Ammanford, SA18 3DN

Telephone number: **01269 597 677**

This person is referred to as the “Responsible Person” throughout this policy.

* 1. This policy requires staff to ensure that the Responsible Person is consulted before any significant new information processing activity is initiated to ensure that relevant compliance steps are addressed.
	2. The Responsible Person is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy or other comments you should contact the Responsible Person. In particular, staff **must always** contact the Responsible Person in the following circumstances:
		1. It is unclear which lawful basis should be relied upon to process personal information (including the legitimate interests used by the MS (see section 5.2 below);
		2. It is necessary to rely on the consent lawful basis to process personal information and/or explicit consent condition to process special category personal information, for automated decision-making or for making cross border data transfers (see section 13 below);
		3. It is necessary to draft a privacy notice (see section 5.5 below);
		4. If the retention period for the personal information being processed is unclear or unknown (see section 9 below);
		5. It is unclear what security or other measures need to be implemented to protect personal information (see section 10 below);
		6. Personal information is being transferred outside the UK (see section 14 below);
		7. If there has been a personal information breach (section 18 below);
		8. Whenever there is a significant change in processing activity or new processing activity in relation to personal information (this may require a Data Protection Impact Assessment) (see section 12 below);
		9. It is intended that personal information will be used for a purpose other than what it was collected for.
1. Definitions
	1. In this policy:
		1. **Personal information** means information relating to identified or identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, constituents, suppliers and marketing contacts. This includes expression of opinion about the individual and any indication of someone else’s intentions towards the individual.
		2. **Special category personal information** means information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sex life, sexual orientation, biometric or genetic data. Personal information relating to criminal offences and convictions should also be treated as special category personal information.
		3. **Processing** means any activity that involves the use of personal information. It includes obtaining, recording or holding the information, or carrying out any operation or set of operations on the information including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal information to third parties.
2. General principles
	1. The MS’s policy is to process personal information in accordance with the applicable data protection laws and rights of individuals as set out below. This Data Protection Policy explains the MS’s procedures for ensuring compliance with the applicable data protection laws. All staff have personal responsibility for the practical application of this Data Protection Policy.
	2. The MS’s office will ensure all processing of personal information complies with the following principles in respect of the processing of personal information, ensuring that personal information is:
		1. Processed lawfully, fairly and in a transparent manner (‘Lawfulness, Fairness and Transparency’).
		2. Collected only for specified, explicit and legitimate purposes (‘Purpose Limitation’).
		3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (‘Data Minimisation’).
		4. Accurate and where necessary kept up to date (‘Accuracy’).
		5. Not kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the information is processed (‘Storage Limitation’).
		6. Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (‘Security, Integrity and Confidentiality’).
	3. The MS’s office must be able to demonstrate compliance with the data protection principles listed above (the ‘Principle of Accountability’).
3. Lawfulness, Fairness and Transparency
	1. Personal information must be processed lawfully, fairly and in a transparent manner in relation to the individual.

**Lawfulness**

* 1. Staff should ensure that there is a legal basis for processing personal information. The legal bases for processing personal information are as follows:
		1. the individual has given their consent (see 13 below);
		2. the processing is necessary for the performance of a contract with the individual;
		3. to meet the MS’s legal compliance obligations;
		4. to protect the individual's vital interests;
		5. for the performance of a task in the public interest;
		6. to pursue the MS’s legitimate interests, where these interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual(s). Reliance on this legal basis will require a Legitimate Impact Assessment to be undertaken and the purposes for which the MS processes personal information for legitimate interests need to be set out in the privacy notices (see section 5.5 below).
	2. If staff are unsure what legal basis is applicable to the personal information they are processing they should contact the Responsible Person.
	3. The processing of special category personal information (see section 3.1(b) above) will require a separate condition for processing. For constituency casework the additional legal basis will usually be that processing the special category personal information will be necessary for reasons of substantial public interest. This is because the processing will be carried out by the MS in their capacity as an elected representative, in connection with the discharge of their functions, and is in response to a request by the individual to take action or a request on the individual’s behalf. Staff should contact the Responsible Person for more information regarding the appropriate condition for processing special category information.

**Fairness & Transparency (Privacy Notices)**

* 1. Data protection law requires the MS to provide detailed, specific information to individuals about how and why their personal information is being processed. Such information must be provided through appropriate privacy notices.
	2. Privacy notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.
	3. Whenever the MS collects personal information directly from individual, the individual must be provided with a privacy notice containing all the information required by data protection law (including the identity of the data controller, how and why the MS will use, process, disclose, protect and retain that personal information). The privacy notice will also make it clear what legal basis is being relied upon and the additional appropriate legal basis if special category personal information is being processed. The privacy notice must be provided when the individual first provides the MS with the personal information. The MS’s general privacy notice for constituents will usually be appropriate in relation to general casework purposes for which the MS collects personal information. Staff should provide the individual with a link to this privacy notice or provide them with a hard copy at the point that the personal information is collected.
	4. When personal information is collected indirectly (for example, from a third party or publicly available source), the individual must be provided with a privacy notice including all the information required under data protection law, as soon as possible, after collecting/receiving the information, but no later than the first communication with the individual or 1 month from receiving the personal information (whichever is earlier), unless this proves impossible or would involve disproportionate effort.
	5. As in section 5.7 above the MS’s general privacy notice will usually be appropriate in relation to constituents. Staff should provide the individual with a link to this privacy notice or provide a hard copy in the first communication or within one month of receiving the personal information, whichever is earlier. Staff should inform the Responsible Person if this is likely to prove impossible or involve disproportionate effort.
	6. Staff are required to include a link to the MS’s privacy notice in their e-mail signature.
	7. Staff must also check that the personal information was collected by the third party in accordance with data protection law and on a basis which contemplates the MS’s proposed processing of that personal information.
	8. Staff should contact the Responsible Person if it is necessary to draft a privacy notice or if they are unclear as to when a privacy notice is required.
1. Purpose limitation
	1. Personal information must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. This is particularly important when dealing with special category personal information which is being processed for casework activities.
	2. Staff cannot use personal information for new, different or incompatible purposes from those disclosed when the personal information was first obtained, unless staff have informed the individuals of the new purposes and legal basis being relied upon (if this legal basis is consent, appropriate consent must be obtained (see section 13 below). For example, the personal information of constituents must not be used for the purposes of political campaigning unless consent has been sought from the individual. Personal information provided in engagement activities which are funded by the Senedd Commission for party political or campaigning purposes must not be shared with a third party.
2. Data minimisation
	1. Personal information must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
	2. Staff may only process personal information when performing their job duties requires this. Excessive personal information should not be collected and staff should ensure, to the best of their abilities, that any personal information collected is adequate and relevant for the intended purposes.
	3. If any personal information is revealed as part of case work activities staff should consider whether the special category personal information is relevant to the matter. If it is not then the special category personal information should be redacted.
	4. Staff must ensure that when personal information is no longer needed for specified purposes, it is deleted or anonymised in accordance with the appropriate retention periods (see section 9 – storage limitation).
3. Accuracy
	1. Personal information must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. This is particularly important when dealing with special category personal information which is being processed for casework activities.
	2. Staff will ensure that the personal information the MS uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it is collected. Staff must check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Staff must take all reasonable steps to destroy or amend inaccurate or out-of-date personal information.
	3. Staff must ensure that personal information held by the MS relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the MS so that records can be updated.
4. Storage limitation (data retention)
	1. Staff must not keep personal information, in a form which permits the identification of an individual, for longer than needed for the legitimate purpose or purposes for which the MS originally collected it.
	2. Staff should ensure personal information is deleted, after a reasonable time, when it is no longer required for the purposes for which it was being held.
	3. The MS has in place a Retention and Erasure Policy setting out the periods for which personal information, including special category personal information should be retained. Any special category personal information provided in connection with casework activities must be considered to establish its relevance. If it is not relevant, then the special category personal information must be redacted. If it is relevant, then the relevance should be reviewed regularly, and the special category personal information redacted when it is no longer relevant.
	4. Staff will take all reasonable steps to destroy or erase from the MS’s systems all personal information that is no longer required in accordance with section 9.2 above. This includes requiring third parties to delete such information where applicable.
	5. Staff will ensure individuals are informed of the period for which information is stored and how that period is determined in any applicable privacy notice (see 5.5 - 12).
5. Security integrity and confidentiality
	1. Personal information must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
	2. The MS has implemented reasonable and appropriate security measures against unlawful or unauthorised processing of personal information and against the accidental loss of, or damage to, or destruction of personal information.
	3. The MS’s office will maintain information security by protecting the confidentiality, integrity and availability of the personal information, defined as follows:
		1. Confidentiality means that only people who have a need to know and are authorised to use the personal information can access it. Where special category personal information is processed, particular consideration must be given as to whether additional confidentiality measures are necessary, such as whether access to the special category personal information should be further limited.
		2. Integrity means that personal information is accurate and suitable for the purpose for which it is processed.
		3. Availability means that authorised users are able to access the personal information when they need it for authorised purposes.
	4. The MS’s office will develop, implement and maintain safeguards appropriate to:
		1. the size of the operation, scope and nature of the processing;
		2. the available resources;
		3. the amount of personal information owned or maintained on behalf of others; and
		4. identified risks (including use of encryption and pseudonymisation (i.e. replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the information relates, cannot be identified without the use of additional information which is meant to be kept separately and secure) where applicable).
	5. The MS’s office will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal information.
	6. Staff have a responsibility for protecting the personal information the MS holds.
	7. Staff must exercise particular care in protecting special category personal information from loss and unauthorised access, use or disclosure.
	8. Staff must follow all procedures in place to maintain the security of all personal information from the point of collection to the point of destruction. Staff may only transfer personal information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested (see sections 14 and 15 below).
	9. Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained in accordance with data protection law and relevant standards to protect personal information.
6. Accountability
	1. The MS’s office must implement appropriate technical and organisational measures to ensure compliance with data protection principles (set out in section 4.2 above). The MS is responsible for, and must be able to demonstrate, compliance with the data protection principles.
	2. The MS’s office must have adequate resources and controls in place to ensure and to document data protection law compliance including:
		1. appointing a staff member with responsibility for data protection compliance;
		2. implementing data protection by design and default when processing personal information to ensure compliance with applicable data protection laws (see section 12 below);
		3. completing Data Protection Impact Assessments (DPIAs) to identify and reduce risks of a processing activity prior to processing, where processing is likely to result in a high risk to rights and freedoms of individuals. DPIAs should be conducted for all major system or business change programs involving the processing of personal information particularly those involving new initiatives or technology (see section 12 below);
		4. integrating data protection into internal documents, policies and procedures including this Data Protection Policy;
		5. regularly training staff on applicable data protection law, this Data Protection Policy, related policies and data protection matters including, for example, individual rights, consent, legal bases, DPIAs and personal information breaches; and
		6. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.
7. Privacy By Design and Data Protection Impact Assessment (DPIA)
	1. The MS’s office is required to implement privacy by design when processing personal information by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.
	2. The MS’s office must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal information by taking into account the following:
		1. the state of the art (i.e. the highest level of general development, as of a device, procedure, process or technique achieved at the particular time);
		2. the cost of implementation;
		3. the nature, scope, context and purposes of processing; and
		4. the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.
	3. The MS’s office mustconduct DPIAs in respect of processing which is likely to result in a high risk to the rights and freedoms of individuals (for example where processing involves special category personal information on a large scale).
	4. Staff should contact the Responsible Person and conduct a DPIA when implementing major system or business change programs involving the processing of personal information including but not limited to:
		1. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
		2. automated processing including profiling and automated decision making;
		3. large scale processing of special category personal information; and
		4. large scale, systematic monitoring of a publicly accessible area (for example, under CCTV).
	5. A DPIA must include:
		1. a description of the processing, its purposes and the MS’s legitimate interests if appropriate;
		2. an assessment of the necessity and proportionality of the processing in relation to its purpose;
		3. an assessment of the risk to the rights and freedoms of individuals; and
		4. the risk mitigation measures in place and demonstration of compliance.
	6. Further guidance in relation to when a DPIA is required and a template DPIA is available from the Information Commissioner’s Website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
8. Consent
	1. The MS must ensure personal information is processed on the basis of one or more of the lawful bases set out in section 5.2 above, one of which is consent. Consent should not be relied upon as the legal basis for processing if another more appropriate legal basis applies.
	2. In order for an individual to validly consent to the processing of their personal information, that consent must be freely given, specific, informed and be an unambiguous indication of the individual’s wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of personal information relating to them.
	3. Consent requires *affirmative* action so silence, pre-ticked boxes or inactivity are not sufficient.
	4. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.
	5. Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if the MS intends to process personal information for a different and incompatible purpose which was not disclosed when the individual first consented.
	6. Consent should not usually be relied upon where there is an imbalance in the relationship between the individual and the MS for example in the context of an employer/employee relationship.
	7. Explicit consent is usually required for:
		1. Processing special category personal information (although staff should contact the Responsible Person to determine the most appropriate legal basis for processing special category personal information).
		2. Automated decision-making; and
		3. Cross border transfers.
	8. Explicit consent requires a very clear and specific statement of consent from the individual (that is, not just action) and the individual should be provided with detailed information in relation to the specific purpose for which explicit consent it being sought.
	9. Where personal information is provided to the MS by the third party and this contains special category personal information relating to the individual, staff must ensure that explicit consent of the individual is evidenced by the third party, or alternatively must ensure that one of the following circumstances apply:
		1. in the circumstances, consent to the processing cannot be given by the individual (potentially because they are ill or otherwise incapable of providing consent);
		2. in the circumstances, it cannot reasonably be expected for the MS to obtain the consent of the individual (potentially because this is a group issue being raised on behalf of a large number of individuals);
		3. obtaining the consent of the individual would prejudice the action taken by the MS (potentially because the action needs to be kept confidential);
		4. the processing is necessary in the interests of another individual and consent has been withheld unreasonably.
	10. Staff must keep records of all consents so that the MS can demonstrate compliance with consent requirements.
9. Limitations on transfers
	1. Data protection law restricts transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals is not undermined. Personal information is transferred from the originating country across borders when it is transmitted, sent, viewed or access in a different country.
	2. The MS’s office may only transfer personal information outside the UK if one of the following conditions applies:
		1. the transfer is based on an adequacy regulation;
		2. appropriate safeguards are in place such as standard data protection clauses (authorised by the Information Commissioner), an approved code of conduct or an approved certification mechanism;
		3. the individual has provided explicit consent to the proposed transfer after being informed of any potential risks; or
		4. the transfer is necessary for one of the other reasons set out under data protection law including the performance of a contract between the MS and the individual, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the individual where the individual is physically or legally incapable of giving consent and, in some limited cases, for the MS’s legitimate interest.
	3. Staff should contact the Responsible Person before transferring personal information outside the UK to ensure one of the conditions outlined above is satisfied.
10. Sharing Personal Information
	1. In general the MS’s office is not allowed to share personal information with third parties unless certain safeguards and contractual arrangements have been put in place.
	2. Staff may only share the personal information held by the MS with another employee, if the recipient has a job-related need to know the information.
	3. Where the MS uses an organisation to process personal information on its behalf, additional security arrangements need to be implemented in contracts with that organisation to safeguard the security of personal information.
	4. Staff should consult the Responsible Person to discuss the necessary steps to ensure compliance when setting up any new arrangement or altering any existing arrangement.
11. Individuals rights and requests
	1. Individuals have rights when it comes to how the MS handles their personal information. These include rights to:
		1. receive certain information about the MS’s processing activities in a privacy notice (see section 5.4 above);
		2. request access to their personal information that the MS holds (via a subject access request) (access);
		3. ask the MS to erase personal information if it is no longer necessary in relation to the purposes for which it was collected or processed (erasure);
		4. to rectify inaccurate information or to complete incomplete information (rectification);
		5. to restrict processing in specific circumstances (restriction);
		6. in limited circumstances, receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine-readable format (data portability);
		7. withdraw consent to processing at any time;
		8. prevent the MS’s use of their personal information for direct marketing purposes;
		9. to challenge processing which has been justified on the basis of the MS’s legitimate interests or in the public interest;
		10. request a copy of an agreement under which personal information is transferred outside of the UK;
		11. object to decisions based solely on automated processing (i.e. when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual);
		12. prevent processing that is likely to cause damage or distress to the individual or anyone else;
		13. be notified of a personal information breach which is likely to result in high risk to their rights and freedoms; and
		14. make a complaint to the Information Commissioner’s Office.
	2. Staff must immediately forward any request received in relation to the rights outlined above to the Responsible Person. This is particularly important because the MS must respond to a valid request within the legally prescribed time limits (under the UK General Data Protection Regulation in the majority of circumstances this is one month from the day the request is received).
12. Political Campaigning/Direct marketing
	1. Providing a political view in order to gain support from an individual is “direct marketing”.
	2. The MS is subject to certain rules and privacy laws when undertaking political campaigning/marketing to constituents or other individuals.
	3. Prior consent is required for electronic direct marketing (for example, by email, text or automated calls).
	4. The right to object to direct marketing (i.e. opt-out, or unsubscribe) must be explicitly offered to the individual in an intelligible manner so that it is clearly distinguishable from other information, when their personal information is collected and in every subsequent communication.
	5. An individual's objection to direct marketing must be promptly honoured. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.
13. Reporting a Personal Information Breach
	1. Data protection law requires the MS to notify personal information breaches to the Information Commissioner’s Office and individual data subjects, in certain circumstances.
	2. Staff should be aware that a personal information breach is any act or omission that compromises the security, confidentiality, integrity or availability of personal information or the physical, technical, administrative or organisational safeguards that the MS or third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal information is a personal information breach.
	3. If staff know or suspect that a personal information breach has occurred, they should not attempt to investigate the matter themselves. Staff should immediately contact the person or team designated as the key point of contact for personal information breaches, namely the Responsible Person.
	4. Staff should ensure that they preserve all evidence relating to the potential personal information breach.
14. Consequences of failing to comply
	1. The MS takes compliance with this Data Protection Policy very seriously. Failure to comply puts both staff and the MS at risk. The importance of this Data Protection Policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.
	2. The MS reserves the right to change this Data Protection Policy at any time without notice. Staff should ensure that have the latest copy of this Data Protection Policy.
15. Review of this Policy
	1. This Data Protection Policy was last reviewed on **30.05.22.**
16. Acknowledgement of receipt and review
	1. I, **[EMPLOYEE NAME]**, acknowledge that on **[DATE]**, I received and read a copy of **[NAME OF MEMBER OF THE SENEDD’s]** Data Protection Policy, dated **[EDITION DATE]** and understand that I am responsible for knowing and abiding by its terms. I understand that the information in this Data Protection Policy is intended to help staff work together effectively on assigned job responsibilities and assist in the use and protection of personal information. This Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed ……………………………………………………….

Printed Name ……………………………………………….

Date ………………………………………………………….