Data Protection policy

This policy provides information about the data protection legislation, including the UK General Data Protection Regulation ('UK GDPR') and Data Protection Act 2018 with which Wales Council for Voluntary Action ('we', 'our', 'us') must comply.

This policy applies to all members of staff, trustees, volunteers and others who do work for us.

This policy provides a general overview of the legal requirements. It sets out what we expect from you in general terms when handling personal information, regardless of the format in which it is stored. This includes information about:

- Current or former employees and workers and applicants
- Current or former volunteers and applicants
- Current or former trustees and applicants
- Beneficiaries/clients/users of our services
- Users of our online and digital media channels
- Current, former or potential supporters, donors and funders including individuals and representatives of organisations
- People with whom we engage in relation to our campaigning activity
- Representatives of organisations with whom we have partnerships or we are collaborating
- Representatives of our suppliers

You must read, understand and comply with this policy when handling personal information on our behalf and attend any compulsory training on its requirements. The policy may be supplemented by specific guidance relevant to your role.

Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

1. DEFINITIONS

The following definitions are used in this policy:

Controller	means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in our organisation for our own purposes
Data Subject	means a living, identified or identifiable individual about whom we hold Personal Data
Data Privacy Impact Assessment (DPIA)	means a tools and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of Personal Data
Data Processors	means any third parties who we use to Process Personal Data on our behalf
Data Protection Officer (DPO)	means the person with responsibility for data protection compliance within our organisation. The current person is Matthew Brown, Director of Operations
Personal Data	means any information identifying a Data Subject or information relating to a Data Subject form which we can identify (directly or indirectly) a Data Subject whether from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special category Personal Data and Pseudonymised

	Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
Personal Data Breach	means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach
Privacy by Design	means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation
Privacy Notice	means a notice setting out information that should be provided to Data Subjects when we collect information about them
Processing or Process	means any activity that involves the use of Personal 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, erasing or destroying it. processing also includes transmitting or transferring Personal Data to third parties
Pseudonymisation or Pseudonymised	means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be

	identified without the use of additional information which is meant to be kept separately and secure
Special Category Personal Data	means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and relating to criminal offences and convictions

2. DATA PROTECTION PRINCIPLES

The law requires that Personal Data must be:

- processed lawfully, fairly and in a transparent manner
- collected only for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- accurate and where necessary kept up to date
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed
- 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.

Personal Data must also not be transferred outside WCVA without appropriate safeguards being in place.

We are required to enable Data Subjects to exercise certain rights in relation to their Personal Data.

We must also comply with particular legal requirements when suppliers that carry out services for us have access to Personal Data and when we are working with organisations and need to share Personal Data.

We are responsible for and must be able to demonstrate compliance with the requirements under the law (accountability).

3. LAWFULNESS AND FAIRNESS

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The law restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The lawful bases available when processing non-special category personal data are:

- the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes
- the processing is necessary for the performance of a contract between us and the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract
- the processing is necessary for compliance with a legal obligation to which we are subject
- the processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- the processing is necessary for the performance of a task carried out in the public interest
- the processing is necessary for the purposes of legitimate interests we are pursuing or which a third party is pursuing, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, in particular where the Data Subject is a child.

A range of additional legal requirements apply when processing special category personal data. One of the lawful basis identified above is required as well as a separate lawful basis from the following list:

- the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

- processing relates to personal data which are manifestly made public by the data subject

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

- processing **is necessary for reasons of substantial public interest,** on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the

management of health or social care systems and services **on the basis of Union or Member State law or pursuant to contract** with a health professional and subject to the conditions and safeguards referred to in paragraph 3

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

    - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

4. TRANSPARENCY

The law requires us to provide detailed, specific information about our use of Personal Data to Data Subjects. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with information including who we are and how and why we will Process, disclose, protect and retain their Personal Data. This is done through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with the Privacy Notice information as soon as possible but no later than one month after collecting/receiving the data. We must also check that the

Personal Data was collected by the third party in accordance with law and on a lawful basis which contemplates our proposed Processing of that Personal Data.

5. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and there is a lawful basis for doing so.

6. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only collect Personal Data that you require for your duties: you should not collect excessive data. You should ensure any Personal Data collected is adequate and relevant for the intended purposes.

7. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You should ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You should check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to amend inaccurate or out-of-date Personal Data.

8. RETENTION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will

maintain retention policies and procedures to ensure Personal Data is deleted in accordance with this requirement.

9. SECURITY

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

You are responsible for protecting the Personal Data we hold.

You may only Process Personal Data when required to do so as part of your role. You cannot Process Personal Data for any reason unrelated to your role.

You must ensure that you follow all guidelines issued to you that are designed to protect against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care to protecting Special Category Personal Data from loss and unauthorised access, use or disclosure.

10. REPORTING A DATA BREACH

The law requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office (ICO) and, in certain instances, the Data Subject.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You should follow the Personal Data Breach reporting policy in Annex 1.

11. TRANSFER LIMITATION

The law restricts data transfers to countries outside the European Economic Area (EEA) where they do not have adequate data protection laws. If you need to send Personal Data outside the EEA, you should contact the DPO for advice.

12. DATA SUBJECT RIGHTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- where processing is based on the lawful basis of consent, to withdraw consent to processing at any time
- receive certain information about our processing activities
- request access to their Personal Data that we hold
- prevent our use of their Personal Data for direct marketing purposes
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- restrict processing in specific circumstances
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- be notified of a Personal Data breach which is likely to result in high risk to their rights and freedoms; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

You must immediately forward any Data Subject request you receive to the DPO.

13. SHARING DATA

You may only transfer Personal Data to third-party service providers who agree to comply with our policies and procedures and who agree to put adequate security measures in place, as requested. We must have a written data processing agreement in place with any such service providers we are using.

In addition, although it is not a legal requirement, it is good practice to have a data sharing agreement with any partners with which we are working that deals with sharing Personal Data. It is essential that you have a clear lawful basis for sharing Personal Data with such partners and that you transmit the Personal Data securely.

14. DEMONSTRATING COMPLIANCE

The law requires us to keep full and accurate records of all our processing activities. You should ensure that any processing of Personal Data that you undertake is included in the records by checking with the DPO.

We are required to ensure all people who work for us have undergone adequate training to enable them to comply with data privacy laws.

We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Data controllers must also conduct DPIAs in respect to high risk processing. If you believe processing that you are carrying out is high risk, please speak to the DPO.

We must also regularly test our systems and processes to assess compliance. You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

REVIEW

March 2022 (Review date: March 2024)

WCVA – Head Office
One Canal Parade
Dumballs Road
Cardiff
CF10 5BF
Tel: 0300 111 0124
Email: help@wcva.cymru

www.wcva.cymru

REPORTING A DATA BREACH

The UK GDPR puts a duty on organisations to report certain types of personal data breaches to the relevant supervisory authority (the ICO). This must be done within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms and individuals must be informed without undue delay.
A decision to report a data breach, either to the Information Commissioner's Office (ICO) or to the data subjects themselves, remains solely with WCVA's Data Protection Officer (DPO).

It is the duty of all staff to report data breaches to the DPO as soon as they become aware of a breach, or in the absence of the DPO, the breach should be reported to the CEO. Awareness is defined as when a member of staff has a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised.

A personal data breach can be categorised as:
'Confidentiality breach' – where there is an unauthorised or accidental disclosure of, or access to, personal data
'Availability breach' - where there is an accidental or unauthorised loss of access to, or destruction of, personal data
'Integrity breach' – where there is an unauthorised or accidental alteration of personal data
It should also be noted that, depending on the circumstances, a breach could concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

You will find below some fictional examples to aid you in identifying data breaches, the notification process that the DPO follows and additional information relating to the scenario presented.

EXAMPLE	DPO TO NOTIFY SUPERVISORY AUTHORITY (ICO)?	DPO TO NOTIFY THE DATA SUBJECT?	COMMENTS
Personal data is on an encrypted USB stick. The USB stick is stolen during a break in.	No	No	As long as the data is encrypted with a 'state of the art algorithm' (this is encryption to AES256 standards for providing personal information) and the unique key is not compromised, this is not a reportable breach.
Personal data is removed from a secure web site managed by WCVA during a cyberattack.	Yes. DPO will report to the ICO and will identify if there are any potential consequences to individuals.	Yes. DPO will inform individuals depending on the nature of the personal data affected and the potential consequences to them.	Even if the risk is deemed as 'not high' to individuals, the DPO may still opt to inform the data subjects of the breach as this initial disclosure may result in additional confidentiality breaches elsewhere.
A ransomware attack takes place that results in data being encrypted. No backups are available, and the data cannot be restored. After investigation, it becomes clear that only encryption took place and no other malware was present.	Yes	Yes. Only the individuals affected need to be notified where there is positive, clear, affirmation that others remained unaffected.	If there was a backup available and data could be restored in good time then this would not need to be reported, as there would be no permanent loss. However, the ICO may consider an investigation to assess compliance in a broader sense. It should however be recorded as an incident by the data protection team on the group's central records.
An individual has received communication from WCVA containing personal data of someone else. Within the initial 24 hour investigation, it becomes clear that a personal data breach has occurred and that other individuals may be affected.	Yes	Yes. Only the individuals affected need to be notified where there is positive, clear, affirmation that others remained unaffected.	If after further investigation, it is found that more individuals are affected then the DPO shall update the ICO accordingly. The DPO may, in certain circumstances, have to notify other individuals if the level of risk to them has increased following the investigation.
A cyber-attack occurs where usernames, passwords and other personal details are published online by the attacker.	Yes	Yes. This is defined as high risk to the individuals themselves.	Password resets should be enforced on the affected accounts with a view to extend this to all users should the risk be determined as possible. Other steps must be employed to mitigate the risk to the affected individuals wherever possible.

Page Break

EXAMPLE	DPO TO NOTIFY SUPERVISORY AUTHORITY (ICO)?	DPO TO NOTIFY THE DATA SUBJECT?	COMMENTS
A website hosting company for the group identifies an error in the code that controls user authentication. The effect means that any user can access any account details.	Yes. The website hosting company must notify its affected clients without undue delay. The website company must inform the group of the data breach and the actions already taken. It is then the group's responsibility to inform the ICO of the data breach.	Yes. By both the website hosting company (where applicable) and the group themselves, where the risk is determined as high.	In this instance, the website hosting company is a processor for the group (as controller), they have a responsibility to the data subject to inform them of the breach and this responsibility would already have been detailed to them in the third party data processing agreement with the group. The group also has a responsibility to inform the individuals as it may cause reputational damage.
Personal data of 5,000 staff are mistakenly sent to the wrong mailing list with 1,000+ recipients.		Yes. DPO will inform individuals depending on the scope and type of personal data involved and the severity of possible consequences.	This would be classed as reckless handling of data; all efforts would need to be employed to mitigate further risks to the rights and freedoms of the data subjects themselves.
A direct marketing email is sent to recipients in the 'to' field rather than the 'bcc' field thereby enabling each recipient to see the email address of other recipients.	Yes. Further action may be needed if a large number of data subjects are affected, special categories of data disclosed, or another high risk is identified *eg* usernames and passwords.	Yes. DPO will inform individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification to the data subjects may, in certain circumstances, not be necessary *eg*, if no special categories of data are disclosed or if the numbers affected remain low. Circumstances may change as the investigation progresses, the option to inform the data subjects may also have to be reviewed later in the investigation.