Personal Data Protection Policy

Version No.: 1.0

Effective From: 1 December 2021

Review Date: 1 December 2023

Signature:	Signed by:	Position:	Date:

1 Introduction

Wansbeck Valley Food Bank (WVFB) uses personal data in the course of providing services, employing staff, recruiting volunteers, communicating with supporters and partners, and coordinating volunteer activities. WVFB respects people's rights to privacy and to protection of their personal data. WVFB is committed to compliance with Data Protection legislation (defined below). This policy sets out WVFB's overall approach to meeting these legal and contractual requirements. Some information is presented in Annexes which form part of the policy.

2 Scope

This policy applies to all processing of personal data by WVFB which completely or partly involves:

• manual filing systems.

• automated means, such as computers.

3 Definitions (see Annex A for further detailed definitions)

Personal Data – the set of personal data gathered from data subjects by the data controller. Under UK-GDPR "personal data" means any information relating to an identified or identifiable natural person ("data subject"); either directly or indirectly from that data (or from that data combined with other information in your possession). Personal data can be factual (for example, a name, address, email address. telephone number. date of birth) or can be a less obvious form of personal information, for example IP addresses or unique device identifiers. Personal data can also be an opinion about that person, their actions or behaviour and can refer to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Sensitive personal data – data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Subject – the natural person to whom the personal data refers.

Data Controller – (also referred to as “the controller“) is the natural or legal person, who determines the purposes and means for processing personal data, i.e.:

• The personal data to be gathered;

• The processes that impact the personal data;

• The third parties with whom the personal data may be shared. Data Processor - (also referred to as "the processor") is the natural or legal person, in this case WVFB, which engages in the processing of personal data on behalf of a data controller.

Natural Person – (also referred to as the "data subject") is a living identifiable person.

Legal Person – is a legal entity or representative of a legal entity; data protection does not apply to information about legal entities (such as corporations, foundations and institutions) or their representatives.

5 Responsibilities of Staff and Volunteers

Everyone who works for or with WVFB shares responsibility for ensuring data is collected, stored and handled appropriately. Staff and volunteers must comply with this policy as well as any supporting procedures and guidance relating to their role. Participation in relevant training is mandatory. Failure to comply will result in disciplinary action.

5.1 Trustees

The Board of Trustees is ultimately responsible for ensuring that WVFB meets its legal obligations in relation to data protection.

5.2 Admin Trustee

The Admin Trustee is responsible for:

• keeping the Board up to date on its data protection responsibilities, risks and issues;

• reviewing data protection policies and procedures;

• arranging training and handling questions from employees and others covered by this policy;

• dealing with requests from individuals for information on data held by WVFB;

• checking and approving contracts or agreements under which third parties may process personal data on behalf of WVFB;

- approving any data protection statements attached to communications; where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

The Admin Trustee is responsible for IT systems and issues, including:

• ensuring all 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 which the company is considering using to store or process data, such as cloud computing services.

5.3 Staff and volunteers

Staff and volunteers should be familiar with, and comply with, the WVFB Data Protection and Security Guidelines set out in Annex J.

Staff and volunteers should note that the following legal offences may result in police action:

• obtaining, retaining or disclosing personal data without consent of the data subject

• selling such personal data or advertising the sale

• re-identifying information that is de-identified personal data without consent of the data subject

• processing such personal data without consent of the data subject

• to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive, under the data subject's right of access and right to data portability

• requiring individuals to provide access, via their right of subject access, to health records, records relating to convictions or cautions, records relating to imprisonment or Disclosure and Barring Service records in connection with the recruitment or employment of a person, a contract for the provision of services, or as a condition of providing goods or services where there is no legitimate reason for requiring this access.

6. Data Protection Principles

Data Protection Legislation is underpinned by the following important principles. These principles say that personal data must be:

• processed fairly, lawfully and in a transparent manner;

• collected only for specific, explicit and legitimate purposes;

• adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected;
• accurate and kept up to date;

• not kept for longer than necessary for the purpose for which the data is collected and for the purposes of complying with our record retention obligations set out in this policy; and

• processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

WVFB is responsible for and must be able to demonstrate compliance with these principles. WVFB will process personal data in compliance with the Data Protection Principles and will maintain records to demonstrate compliance (see Section12 ‘Record Keeping’).

Staff and volunteers are expected to apply the Data Protection Principles below in the context of their role

6.1 Lawfulness, fairness and transparency

WVFB will process personal data in a lawful, fair and transparent manner. WVFB will ensure that data subjects receive information about WEFB in its role as data controller and the purposes of processing. WVFB will use clear and plain language in the form of Privacy Statements to communicate with data subjects and ensure that information about processing of personal data is easily accessible and easy to understand.

In designing its processes, WVFB will establish the lawful basis for any processing of personal data. Conditions for lawful processing are summarised in Annex B.

In the case of sensitive personal data (see Annex A), WVFB will identify additional justification for lawful processing. Legal criteria for processing sensitive personal data are shown in Annex C.

WVFB will consider the detailed requirements of the legislation and regulations where clarification is required.

6.2 Purpose limitation

WVFB will collect personal data only for specified, explicit and legitimate purposes and will not further process the data for incompatible purposes. WVFB may carry out further processing for the purposes of the public interest, scientific or historical research or statistical purposes.

6.3 Data minimisation

WVFB will only collect personal data to the extent that it is required for the specific purposes for which it is being processed. This purpose will be included in the appropriate Privacy Notices and notified to the individual at the time of collection.

6.4 Accuracy

In respect of the personal information that we control, we will ensure that this is accurate and kept up to date. Bearing in mind our document retention obligations, we will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

6.5 Storage limitation

WVFB will keep personal data in a form that makes it possible to identify data subjects for no longer than is necessary for the purpose or purposes for which it was collected. If data is retained for longer periods for purposes in the public interest, scientific or historical research purposes or statistical purposes, WVFB will safeguard the rights and freedoms of data subjects.

6.6 Integrity and Confidentiality

WVFB will ensure that the manner of processing ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

WVFB will maintain data security by preceding the confidentiality, integrity and availability of the personal data, defined as follows:

(a) confidentiality means that only people who are authorised to use the data can access it.

(b) integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) availability means that authorised users should be able to access data if they need it for authorised purposes. Personal data will therefore be stored, either on WVFB's central computer system or cloud-based storage, not individual devices. Foodbank client data relating to vouchers and food parcels will only be stored on WVFB's central computer system or cloud-based storage.

6.7 Rights of Data Subjects

Legal rights of data subjects are explained in Annex D.

WVFB has a legal responsibility to enable data subjects to exercise their rights.

The law requires data controllers to communicate with data subjects about processing: • in a concise, transparent, intelligible and easily accessible way using clear and plain language.

• by any appropriate means including:

    - orally, when this is requested by the data subject, subject to identity being proven by other means
    - electronically, where personal data are processed by electronic means

- • free of charge, except where requests are clearly unfounded or excessive when a charge may be made to cover administrative costs or the request may be refused.

WVFB has Privacy Notices to explain how WVFB complies with the law and enables data subjects to access their rights. When collecting personal data or advising about rights, staff and volunteers must make the relevant Privacy Notice available to the data subject. The minimum contents of a Privacy Notice are listed at Annex H. WVFB will also include information about its complaints process.

Data subjects are also entitled, in some cases, to request the deletion of the personal information WVFB hold about them.

7 Data access requests

Data Subjects whose personal data we hold are entitled to make a formal request for details of this information. They are entitled to details on the following:

• the categories of data we hold about them;

• the purposes for which we process their data;

• the recipients to whom the personal data has been or will be disclosed;

• the period of time for which we anticipate that the data will be stored;

• the existence of the right to rectify or erase this data;

•the right to lodge a complaint with the Information Commissioner's Office;

• where personal data is not collected from the individual, any available information about where we received their data; and

• in the event personal data is transferred outside of the EEA, the individual has the right to be informed of the appropriate security measures and safeguards in place for the transfer.

Any data access / deletion requests must be made in writing and should be referred to the Admin Trustee immediately for them to coordinate the response. No member of staff or volunteer should attempt to deal with the request themselves.

A data subject may not be charged for their request to access data, unless the request is manifestly unfounded, excessive or repetitive, in which case we may charge a reasonable fee. The Admin Trustee will aim to provide the relevant data as soon as possible and within 30 days of receipt of the request. Where the request is complex we may extend the time for compliance by two months, however we must respond to the individual within 30 days of the initial request explaining that we require the extension.

The Admin Trustee will verify the identity of anyone making a data subject access request (DSAR) before handing over any information. WVFB will give careful consideration to any grounds we may have for refusing disclosure or deletion of personal data held by WVFB, but where there are no grounds for such refusal WVFB will always act in accordance with our obligations under the Data Protection Legislation to the fullest extent possible.

8 Data Controller and Data Processor roles

WVFB may act as a controller, joint controller or processor. The role affects how processes are developed and operated. Legal responsibilities of controllers and processors are listed in Annex E. The respective responsibilities of joint controllers for compliance should be made clear in a formal agreement. Joint controllers bear joint liability in the event of a data breach. A processor should process personal data in accordance with purposes and means determined by the controller. If a processor strays beyond the role by determining purposes and means then the law considers it to be a controller.

8.1 Data protection by design and default

A controller has a duty to

• consider risks including possible impacts on the rights and freedoms of individuals;

• take appropriate technical and organisational measures to protect data subjects and their rights;

• implement these measures to ensure data protection by design and default.

Data processing risks, risk assessment and general approaches to mitigate risk are identified at Annex F. Staff or volunteers who develop processes for personal data should apply the principles for privacy by design presented at Annex G.

9 Data Protection Impact Assessment

WVFB may conduct a data protection impact assessment (DPIA) to identify the origin, nature, specific details and severity of risks.

The law requires a DPIA for:

• automated evaluation of persons;

• large scale processing of sensitive personal data; and

• systematic monitoring of a publicly accessible area on a large scale.

A DPIA must at minimum include:

• systematic description of the processing operations, purposes and, where applicable, the legitimate interest pursued by the controller

• assessment of the necessity and proportionality of the processing operations in relation to the purposes

• evaluation of the risks to the rights and freedoms of data subjects

• possible measures to address risks and demonstrate compliance

Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, a controller must consult the Information Commissioner's Office (ICO) prior to processing.

10 Transferring data outside the European Economic Area

WVFB may transfer personal data to a country outside the European Economic Area (EEA). This will only be done if all the following conditions apply:

• the country to which the personal data is transferred ensures an adequate level of protection for the individuals' rights and freedoms;

• the individual has given their consent;

• the transfer is subject to appropriate safeguards;

• the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims; or

• the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

11 Disclosure and sharing of personal information

WVFB may disclose personal data to third parties if WVFB is under a duty to disclose or share an individual's personal data in order to comply with any legal obligation, including where it is necessary to share such data in order to investigate or prevent fraud, or in order to enforce or perform any contract with the individual or other agreements, or to protect our rights, property, or safety of our employees, clients or others.

12 Record Keeping

WVFB will maintain written records (i.e. a Record of Processing - ROP), which it will make available to the ICO on request, of:

- the names and contact details of relevant controllers and processors
- where WVFB is the data controller:
    - o the purposes of the processing
    - o categories of data subjects, personal data and recipients
    - o envisaged time limits for erasure of the different categories of data
- Where WVFB is the data processor:
    - o Categories of processing carried out on behalf of each controller
- A description of technical and organisational security measures, where possible
- Any transfer of data outside the EEA and related safeguards

13 Complaints

WVFB provides a complaints process which provides for:

- investigation as appropriate;
- updating on progress;
- information on the outcome;
- information on the right to escalate a complaint to the ICO.

14 Dealing with a Data Breach

A data protection breach can happen for a number of reasons including:

- loss or theft of personal data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;

• human error;

• unforeseen circumstances such as a fire or flood; or

• hacking attack

In view of the possible impacts on data subjects, the law sets tight deadlines for notification of breaches. The co-operation of staff and volunteers is vital to achieving these deadlines. A member of staff or volunteer who becomes aware of a data breach must notify the Admin Trustee of WVFB or nominated representative immediately. The Admin Trustee will consider the need for notifications to be made in accordance with Annex I.

15 Working with Data Processors

If WVFB considers hiring or outsourcing personal data processing to a new Processor, it will check whether the Processor has obtained certification to any security-related standard and ask the potential Processor for evidence of their data security procedures.

A contract will be put in place with a new Processor requiring that the Processor will:

• process the personal data only on documented instructions from WVFB

• ensure that persons authorised to process the personal data are committed to confidentiality

• keep the data secure

• not hire another Processor to do the work without permission of WVFB

• help WVFB to fulfil requests from data subjects enforcing their rights

• help WVFB to fulfil legal and regulatory duties including breach notification requirements

• delete or return the personal data at the end of the contract, as required by WVFB

• provide information to demonstrate compliance including allowing their processes to be inspected and audited

16 Succession arrangements

Should WVFB cease to exist or be replaced, document retention obligations continue, particularly in relation to Foodbank clients, and will either transfer to a successor or be permanently deleted. Likewise, should WVFB merge with or take over the responsibilities of another Foodbank it will request that all relevant information, particularly in relation to Foodbank clients, is transferred to the management of WVFB.

17 Equality and Diversity

WVFB is committed to ensuring that it treats its employees and volunteers equitably and reasonably and that it does not discriminate against individuals or groups on the basis of their ethnic origin, physical or

mental abilities, gender, age, religious beliefs or sexual orientation. This policy has been appropriately assessed.

18 Monitoring and Compliance

WVFB will maintain effective monitoring systems to ensure implementation of this policy, including the following:

Standard/process/issue	**Monitoring and audit**			
	Method:	**By:**	**Reporting to:**	**Frequency:**
Training in personal data protection principles and good practice	Annual review with data processors.	Admin Trustee	Trustees	Annually
Regular data backups taken	Check regular backups are made	Admin Trustee	Trustees	Quarterly
Destruction of old personal data and documents	Check that old documents/data destroyed according to retention dates	Admin Trustee	Trustees	Quarterly
Maintain Record Processing (ROP)	Check ROP is up to date	Admin Trustee	Trustees	Annually

19 Amendment Table

Version	**Effective From**	**Date of Review**	**Changes made**

Annexe A

Definitions

"Personal data" means any information about an identified or identifiable living person, called "a data subject". The person might be identifiable directly (by their name or other identifier) or indirectly (through location data and/or other factors specific to the person).

"Sensitive personal data" reveals:

1. racial or ethnic origin
2. political opinions
3. religious or philosophical beliefs
4. trade union membership
5. genetic data
6. biometric data used to identify people (e.g. facial images and voice recordings)
7. health data
8. data concerning individual's sex life
9. sexual orientation

“Filing system” means a structured set of personal data which is accessible according to specific criteria, which may be automated or manual and which may be centralised or dispersed on a functional or geographical basis.

"Processing" means any operation on personal data, whether or not by automated means, such as:

(a) collection, recording, organisation, structuring or storage

(b) adaptation or alteration

(c) retrieval, consultation or use

(d) disclosure by transmission, dissemination or otherwise making available

(e) alignment or combination, or

(f) restriction, erasure or destruction

A "data controller" or "controller" is the natural or legal person who determines the purposes and means for processing personal data.

A "data processor" or "processor" engages in the processing of personal data on behalf of a data controller.

"ICO" means the Information Commissioner's Office. Data controllers and data processors are accountable to the ICO for their data processing.

Annex B

Conditions for lawful processing of personal data

Processing is lawful where at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
• Consent means an indication of the data subjects' wishes that is given freely and is specific, informed and unambiguous. Consent can be granted by a statement or by a clear affirmative action.
• Records to demonstrate consent must be maintained. Where a written declaration is used, the request for consent to processing must be distinguished from any other matters. The request must be presented in an intelligible and easily accessible form and use language which is clear and easy to understand.
• Data subjects may withdraw their consent to future processing at any time. Before a person gives consent, they must be informed about the possibility of withdrawing it. Withdrawing consent must be made as easy as giving it.
• For a child under 13, the request for consent must be made to the parent or legal guardian.

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, 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.

- The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Annex C

Conditions for lawful processing of sensitive personal data

Sensitive personal data may not be processed unless (at least) one of the conditions listed in annex B is met and, in addition, (at least) one of the following conditions applies –
(a) the data subject has given explicit consent, except where law prevents this;

(b) processing is necessary to meet obligations and specific rights relating to employment, social security and social protection law;

(c) 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;

(d) 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;

(e) processing relates to personal data which are manifestly made public by the data subject;

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

(g) processing is necessary for reasons of substantial public interest, on a legal basis and subject to suitable safeguards;

(h) processing is necessary for medical purposes, assessment of working capacity, health and social care, or under contract with a health professional where the processing is under the responsibility of a person who is subject to an obligation of secrecy under law or rules established by national competent bodies;

(i) processing is necessary for reasons of public interest in the area of public health;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to legal safeguards;

Processing of personal data about criminal convictions and offences or related security measures may only be carried out with specific legal authorisation and safeguards.

Annex D

Rights of Data Subjects

Right of access

Data subjects have a right to confirmation of whether or not a data controller is processing their personal data and, if so receive:

- a copy of the personal data
- the purposes of the processing
- the categories of the personal data
- the recipients or categories of recipient of the personal data
- the storage period, or criteria to determine the storage period
- existence of the rights to rectification, erasure, restriction of processing or objection
- the right to lodge a complaint with the Information Commissioner's Office
- any information about the source of the personal data, if not the data subject
- the existence of any automated decision making and information about this
- relevant safeguards, if data is transferred to a third country

If a request to access personal data is made by electronic means, the controller should respond in electronic form unless the data subject specifically requests otherwise. The controller must provide a first paper copy free; for any additional copy, the controller may charge a fee based on administrative costs.

The right to obtain a copy may not adversely affect the rights and freedoms of others.

Right to rectification

Data subjects have the right to:

- rectification of inaccurate information about them without undue delay
- have incomplete personal data completed, including by supplementary statement

Where the data subject has exercised their right to rectification, the controller shall communicate this to each recipient of the personal data (unless impossible or disproportionate effort). The controller shall inform the data subject about those recipients if the data subject requests it.

Right to object

Data subjects have a right to object to further processing of their personal data where the legal basis for the processing is that it is necessary for: tasks performed in the public interest; or the legitimate interests of a data controller or a third party.

In such situations, the controller must indicate the existence of the right to object:

- at the time of the first communication with data subjects
- in a clear manner and separately from other information.

If a data subject exercises the right to object, the controller must cease the processing if there are no compelling legitimate grounds for continuing it and processing is not needed in relation to legal claims.

Right to restriction of processing

Data subjects have a right to obtain restriction of processing from the controller where:

- accuracy of personal data is contested - for a period enabling verification;
- processing is unlawful, and data subjects request restriction rather than deletion;
- controllers no longer need the data for the purposes of the processing but the data are required by data subjects for legal claims;
- data subjects object to the processing pending verification of whether the legitimate grounds of data controllers override those of data subjects.

If one of these conditions applies, the controller may only continue processing:

- with the consent of the data subjects;
- in relation to legal claims;
- for the protection of the rights of others;
- for reasons of important public interest.

Where the data subject has exercised their right to restriction of processing the controller shall communicate this to each recipient of the personal data (unless impossible or disproportionate effort). The controller shall inform the data subject about those recipients if the data subject requests it.

Where a restriction of processing has been obtained, the controller will inform data subjects before the restriction is lifted.

Right to erasure

Data subjects have a right to erasure of their personal data by the controller without undue delay if:

- the data are no longer needed for the relevant purposes;
- data subjects withdraw consent and there is no other legal basis for processing
- data subjects object to processing and there are no overriding legitimate grounds for the processing
- personal data have been unlawfully processed
- personal data must be deleted to comply with a legal obligation
- personal data have been collected in relation to the offer of any service which is normally requested by an individual at a distance via electronic means and paid for.

Where a controller has disclosed data which it obliged to erase, it must take reasonable steps to inform other relevant controllers that the data subject has requested erasure of any links to or copies of the data.

The right to erasure does not apply where processing is necessary:

- to exercise of the right to freedom of expression and information
- to comply with a legal obligation
- for a task carried out in the public interest
- for scientific, historical research or statistical purposes
- in relation to legal claims

Where the data subject has exercised their right to erasure, the controller shall communicate this to each recipient of the personal data (unless impossible or disproportionate effort). The controller shall inform the data subject about those recipients if the data subject requests it.

Annex E

Responsibilities of Data Controllers and Data Processors

Data controllers must:

- implement measures, including appropriate policies, to ensure and demonstrate processing in accordance with the law
- demonstrate its compliance with the data processing principles
- consider the nature, scope, context and purposes of processing and risks including possible impacts on the rights and freedoms of individuals
- take appropriate technical and organisational measures to protect data subjects and their rights, and implement these measures to ensure data protection by design and default
- maintain records of data processing activities to demonstrate legal compliance
- ensure a level of security appropriate to the risk in processing data
- co-operate with the ICO as appropriate and notify the ICO in the event of a breach
- conduct data protection impact assessments where there is high risk
- consider whether there is a requirement to appoint a Data Protection Officer
- meet legal obligations regards transfer of any data outside the EU
- assist data subjects with exercising their rights to privacy and data protection, including providing information when collecting personal data

Data processors must:

- comply with the contract (or similar act) which clarifies the processing details and, as required by the contract,
    - act on written instructions from the data controller

◦ ensure confidentiality, assist the controller to comply with the law and respond to requests from data subjects
◦ provide information to demonstrate compliance of the controller
◦ assist the controller with ensuring security of processing
◦ treat personal data after processing as directed by the controller • comply with the data processing principles

- protect the rights and freedoms of data subjects
- demonstrate compliance with legislation
- maintain records of processing and make them available to the ICO on request
- consider need to appoint a Data Protection Officer
- cooperate with ICO as appropriate
- take appropriate technical and organisational measures to ensure security and protect the rights of data subjects
- meet specific obligations regarding transfer of data outside the EU

Annex F
Data processing risks, risk assessment and general approaches to mitigate risk

Risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored or otherwise processed.

Assessment of the level and impact of risks should include consideration of the volume of personal data, the number of data subjects concerned and the possibility of:

- discrimination
- identity theft or fraud
- financial loss
- damage to reputation
- loss of confidentiality of personal data protected by professional secrecy
- unauthorised reversal of pseudonymisation
- other significant economic or social disadvantage
- damage to data subjects' rights and freedoms or exercise of control over their data
- unauthorised use or disclosure of sensitive personal data or data about vulnerable people and children in particular
- unauthorised use or disclosure of data which may be used for evaluation such as performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements

The approach to mitigating risk should take into account:

- the nature, scope, context and purposes of processing
- the state of the art
- implementation cost
- the likelihood and severity of risks for the rights and freedoms of individuals.

Measures to mitigate risk may include:

- Transparency with regard to the functions and processing of personal data
- Minimisation of the collection, processing and storage of personal data
- Anonymisation – where ways of identifying the data subject are irreversibly destroyed and the data subject cannot be re-identified either directly or indirectly
- Pseudonymisation – where additional data is required to re-identify the data subject: this may include replacement of personal details by a code
- Encryption
- Steps to ensure people acting for controller/processor do not process personal data except on instructions from the controller (except where the law requires)
- Authentication and authorisation mechanisms
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services
- Ability to restore the availability and access to personal data in the event of a physical or technical incident
- Arrangements for confidential disposal and destruction of personal data
- Regularly testing the security measures

Annex G
Seven Foundational Principles for Privacy by Design

1. A ***proactive and preventative approach*** which aims to address risks of invasion of privacy and prevent these rather than on remedies after the event.

2. ***Privacy as the default*** - The purpose for processing the information will be clearly communicated to the person concerned. The collection of information shall be fair, lawful, limited to that purpose and the strict minimum required for that purpose. The processing, storage period and accessibility of the data shall be limited to that purpose and, when that processing is complete, the data shall be destroyed.

3. Privacy ***embedded*** into design – with consideration of privacy risks and measures to mitigate those risks from the outset as an integral part of the development of processes (see annex F).

4. ***Full*** functionality – design which accommodates all legitimate objectives including technical capabilities, privacy and security.

5. ***End to end security*** to assure the confidentiality, integrity and availability of personal data throughout its lifecycle including methods of secure destruction.

6. ***Visibility and transparency*** to verify that processing happens according to stated promises and objectives. This includes clear accountability, making information about policies and practices available, a complaint process and steps to check compliance.

7. ***Respect for user privacy*** – to keep the interests of the individual uppermost during process design. Processes should:

- be user friendly
- enable informed decisions about consent
- maintain accuracy of information
- enable individuals to:
    - access information and be informed about its uses and disclosures
    - challenge the accuracy of the information and have it amended
- communicate opportunities for complaint and redress

Reference

Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices. Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada. https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf Page 20 of 23 A

Annex H

Minimum content for a Privacy Notice

On collecting personal data directly from data subjects, a controller must provide information on:

- The controller's identity and contact details
- The contact details of the person responsible for data protection
- The purposes and legal basis for the data processing
- The reason why the data subject needs to provide personal data, whether the data subject is obliged to provide the data and the consequences of not doing do
- The recipients of the personal data
- Whether the controller intends to transfer personal data outside the EU
- The data storage period
- Data subjects' rights: access, rectification, erasure, restriction of processing, objection to processing, data portability, right to withdraw consent, opportunity to lodge a complaint with WVFB, right to lodge a complaint with the ICO
- The existence of any automated decision making, including profiling

- Whether the controller intends to further process the data for a purpose other than that for which the data is initially collected

If personal data is collected indirectly, the controller must provide data subjects with

- the information listed above
- details of the categories of personal data
- the source.

unless

- the data subject already has the information
- doing so would be impossible or incur disproportionate effort
- doing so would make impossible or seriously impair achievement of the processing objectives
- the law provides measures to protect the legitimate interest of data subjects
- the data is subject to a legal obligation of professional secrecy.

Annex I
Notifications by the Admin Trustee in the event of a Data Breach

A member of staff or volunteer who becomes aware of a data breach must notify the Admin Trustee of WVFB or nominated representative ***immediately***. The Admin Trsutee will then consider the need for notification of the ICO, a data controller and data subjects.

(a) Notification of the ICO

If WVFB is the data controller, it will notify the ICO about a breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. WVFB will make the notification without delay and, where feasible, within 72 hours of becoming aware of it. If notification is not within 72 hours, WVFB will indicate the reasons for the delay. The notification shall include:

- the nature of the breach including, where possible, the categories and approximate number of data subjects and the categories and approximate number of records
- the name and contact details where more information can be obtained
- the likely consequences of the personal data breach
- the measures taken or proposed to be taken to address the breach including any measures to mitigate possible adverse effects

To minimise delay, WVFB may provide this data in phases.
Measures taken to address a breach may include:

- prompt action to mitigate the damage suffered by data subjects
- notification, communication and co-operation with the ICO to remedy the failure and mitigate possible adverse effects
- communication with the data subject
- review of practice to achieve security, data protection by design and default and legal compliance

WVFB will record any such breach including facts relating to the breach, its effects and remedial action taken and make this record available to the ICO to verify compliance.

(b) **Notification of a data controller**

As a processor, WVFB will notify the controller of a breach without undue delay. If WVFB engages a processor, it will require the processor to notify it of breaches without undue delay.

(c) **Notification of data subjects**

If WVFB is the data controller, it will communicate to data subjects in clear, plain and understandable language the same information given to the supervisory authority unless:

- appropriate measures such as encryption have been applied
- subsequent measures prevent high risk to rights and freedoms of data subjects
- disproportionate effort would be required and a public communication or similar measure would be sufficient to inform data subjects.

Annex J
WVFB Data Protection and Security Guidelines

Trustees, staff and volunteers are all responsible for keeping personal data secure, by taking sensible precautions and following the guidelines below:

- **Clear desk policy with secure lockable drawers or filing cabinets.** Desks should be kept clear. Files, laptops and other devices and confidential information of any kind should be locked away overnight. Personal information is always confidential information. Employees and volunteers should make sure paper and printouts containing personal information are not left in general sight, e.g. on a printer. If data is stored on removable media (like a memory stick or DVD), these should be password protected and kept locked away when not being used.
- **Archived files.** Paper files containing personal information which must be retained for regulatory purposes are to be stored in a secure off-site archiving facility. Regular reviews should be undertaken to ensure personal data contained in these files is not being kept for longer than is necessary.
- **Data stored electronically.** Data should be protected by strong passwords that are changed regularly and never shared between employees. Data should only be stored on designated drives and servers, and should only be uploaded to an approved secure cloud computing service. Employees and volunteers should not use personal/home email accounts for transferring personal data relating to WEFB employees, volunteers or clients.
- **Secure servers.** Servers containing personal data are sited in a secure location, and are protected by approved security software and a firewall. Physical or electronic access is limited to those authorised and agreed with the service provider.
- **Ensuring equipment and devices used to access data are secure.** Data should never be saved directly to laptops or other mobile devices like tablets or smartphones. All computers and devices used to store and access data should be protected by passwords, approved security software and a firewall. Users must ensure that individual monitors do not show confidential information to passers-by and that screens are password locked when left unattended.
- **Exercising caution when sharing data**. Data should not be shared informally. Personal data should not be disclosed to unauthorised people, either within the organisation or externally. Employees and volunteers must not access or process data unless it is necessary to do so in the performance of their duties and must always ensure they are acting in accordance with the applicable legislation when carrying out that access and processing. WVFB will have provided training, but if employees or volunteers are unsure about their duties in this respect, they should discuss this with WVFB's Operations Trustee and/or Admin Trustee. If an employee or volunteer suspects they have had access to confidential information or personal data which should not have been shared with them, or if they have shared information with someone who should not have received it, they must speak to the Admin Trustee and/or Operations Trustee immediately in order to decide on the appropriate remedial action.

Electronic Data Storage

WVFB has adopted a 'cloud' based solution to secure data storage. All data is securely held and must meet UK-GDPR data protection and security standards. All documents are filed electronically, with hard copies retained only when required.

Document Retention Periods

WVFB will keep records for the period required by HMRC, any funders, or as required under other statutory or contractual obligations.

- Fulfilled client vouchers will be held for two years
- Company Statutory books are kept for as long as the company remains in existence.
- HMRC required records to be kept for Corporation Tax purposes for 7 years, and VAT records for 4 years. Company policy is to retain all financial records for 7 years.
- Leases and documentation relating to premises owned or rented by WVFB or its subsidiaries must be retained until the lease has expired or been assigned and/or the premises have been sold or transferred from the company's ownership.
- Client files should be labelled to show the retention period applicable to them.

Document Destruction

Documents or files may only be destroyed if retention period has expired and there is no other requirement to keep them. Destruction is authorised by the Admin Trustee.