WFSA data protection manual 2024 Reviewed

Introduction

Purpose

This manual aims to provide a comprehensive overview of the regulatory climate concerning data protection, WFSA's policies and procedures for compliance, and where to find further information.

It aims to ensure that all personnel, employees, volunteers and contractors understand their responsibilities regarding data protection and comply with the relevant legal requirements. By following the guidelines set forth in this manual, we aim to protect the privacy and integrity of the personal data we handle, maintain trust with our stakeholders, and mitigate risks associated with data breaches.

Scope

This manual applies to all staff members, including full-time, part-time, and temporary employees, as well as volunteers and contractors who have access to our data systems. It covers all aspects of data protection, including the collection, storage, processing, and sharing of personal data. This manual is applicable to all data handled by the WFSA, regardless of its format (e.g., electronic, paper) or the location of the data processing.

Contact Information

Please inform Laurie Barnes or Kristine Stave if you notice any omissions, discrepancies between sections, or if you come across any resources that may be useful for us to consider.

Roles and Responsibilities

Role of Employees

All staff members are responsible for ensuring that any personal data they hold is kept securely and is not disclosed to any unauthorised third party. Personal data should only be accessible to those who need it for their work. Employees are integral to the effective implementation of our data protection policies. Please see Appendix 1: Employee acknowledgement.

Their responsibilities include:

- Understanding and complying with the data protection principles and policies outlined in this manual.
- Collecting, processing, and storing personal data in accordance with legal and organisational requirements.
- Ensuring the accuracy and security of personal data they handle.

- Reporting any suspected data breaches or security incidents to Laurie Barnes without delay.
- Attending regular data protection training and staying informed about updates to relevant regulations and policies.

Role of Volunteers

Volunteers play a crucial role in maintaining data protection within our Federation. Volunteers are treated as employees in terms of data protection. They are held to the same standard as the rest of the team and briefed on the importance of keeping data secure and not sharing it outside the organisation.

Their responsibilities include:

- Adhering to the data protection policies and procedures outlined in this manual.
- Ensuring that personal data is handled confidentially and securely.
- Reporting any data breaches or security incidents to Laurie Barnes, or Kristine Stave immediately.

Long-standing programme/project volunteers are given WFSA email accounts to separate data from personal accounts. Whenever possible, volunteers use WFSA computers to prevent data retention on personal devices after their engagement ends. For volunteers who are not using WFSA-provided computers, additional measures must be taken to mitigate the risk of data breaches.

Information relating to the UK-GDPR is included in the Volunteer Handbook and during their induction to WFSA. Volunteers are required to sign a data privacy notice as part of their induction, which is re-visited on an annual basis.

Role of Contractors

Contractors, similar to volunteers, are also treated as employees with respect to data protection. They are expected to adhere to the same data protection policies and procedures and are equally responsible for maintaining the confidentiality and security of personal data. Contractors are briefed on data protection protocols upon their engagement and are required to sign a data privacy

notice, which is reviewed annually. Additionally, contractors must ensure that any data they handle is stored securely and not retained on personal devices or accounts after their contract ends.

Relevant Legislations

PECR (Privacy and Electronic Communications Regulations)

The Privacy and Electronic Communications Regulations (PECR) were established as The Privacy and Electronic Communications (EC Directive) Regulations 2003. These regulations are derived from European law and implement the European Directive 2002/58/EC, also known as the 'e-Privacy Directive.' It applies even post-Brexit. PECR governs all forms of electronic communications, ensuring the privacy and security of such communications.

PECR is particularly relevant to us in the following areas:

Marketing by Electronic Means: Marketing by electronic means refers to any marketing communications sent directly via email or made through calls to an individual. However, routine customer service messages, which provide information needed about a current or past purchase, are excluded from this definition. Also excluded are solicited messages, where individuals actively request information. If someone specifically asks us to send them information, we can do so without concerns about PECR, although we must still identify ourselves, display our number when making calls, and provide a contact address.

Consent Requirement: The general rule under PECR is that we can only send marketing texts or emails to individuals (including sole traders and some partnerships) if they have specifically consented to receive them. This means we need affirmative consent for texts and emails under PECR.

We must keep clear records of exactly what someone has consented to, including:

- The content they consented to.
- The date of consent.
- The method of consent.
- Who obtained the consent.
- The information provided to the person consenting.

Enforcement and Penalties: The Information Commissioner's Office (ICO) has various ways to take action against those who breach PECR, including:

- Criminal prosecution.
- Non-criminal enforcement.

- Audits. The ICO can also issue a monetary penalty notice, imposing fines of up to £500,000. Recent examples of enforcement actions include:
    - **Flybe:** Fined £70,000 for sending 3.3 million emails to past customers in 2016-17 to verify their details.
    - **Honda:** Fined £13,000 for sending emails to clarify customers' preferences for future communications.

In January 2018, 7,680 concerns related to PECR were reported to the ICO, marking a 33% increase from the previous month. In 2020/21, the ICO issued £42 million in fines, a 1580% increase from the previous year, highlighting the public's concern over unsolicited marketing and cold-calling.

UK-GDPR (General Data Protection Regulation)

The General Data Protection Regulation (GDPR) became effective in the UK on 25 May 2018. Enacted through the Data Protection (Amendment) Act, it replaced previous data protection laws (such as the Data Protection Act 1998) and provided individuals with enhanced rights and protections regarding their personal data. With the UK exiting the EU, data protection legislation now includes all regulations in force regulating the use of personal data and the privacy of electronic communications. This includes:

- The retained EU law version of GDPR ((EU) 2016/679), known as the "UK GDPR."
- The Data Protection Act 2018.
- The Privacy and Electronic Communications Regulations 2003 (as amended).
- Any successor legislation.

To comply with the UK-GDPR, organisations must:

- Ensure that data is accurate and up to date. Article 5 of the UK-GDPR mandates that "every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay."
- Respect customers' right to opt-out of marketing. If a customer opts out, businesses must immediately cease all marketing activities to that customer.
- Honour customers' rights to opt-out of automated profiling, which can impact CRM systems and retargeting efforts.
- Address technical issues such as the identification and removal of duplicate customer profiles across multiple databases.

Customers have several rights under the UK-GDPR, including:

- **Right to Data Access:** Customers can request all data held about them, which businesses must provide in an accessible format.

- **Right to Data Portability:** Applies to personal data provided by the individual, processed based on consent or contract, and carried out by automated means.
- **Right to Withdraw Consent:** Customers must be able to easily withdraw consent, just as easily as they gave it.

Roles of Data Controllers and Processors:

- **Data Controllers:** Determine the purposes and means of processing personal data.
- **Data Processors:** Process personal data on behalf of a controller. Processors have specific legal obligations, such as maintaining records of processing activities and being liable for breaches. Controllers are not relieved of their obligations even when a processor is involved and must ensure their contracts with processors comply with the UK-GDPR.

The UK-GDPR applies to processing carried out by organisations operating within the UK, as well as organisations outside the UK that offer goods or services to individuals in the UK.

Data Protection Principles: Article 5 of the UK-GDPR sets out the main responsibilities for organisations:

A. Process personal data lawfully, fairly, and transparently.
B. Collect data for specified, explicit, and legitimate purposes and not process it in a manner incompatible with those purposes.
C. Ensure data is adequate, relevant, and limited to what is necessary.
D. Keep data accurate and up to date; rectify or erase inaccuracies without delay.
E. Store data in a way that permits identification of data subjects for no longer than necessary.
F. Secure personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage.

What this means for us

- We must have a valid lawful basis to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on our purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If we can reasonably achieve the same purpose without the processing, we won't have a lawful basis.
- We must determine our lawful basis before we begin processing, and we should document it. We should not swap to a different lawful basis at a later date without good reason.
- Our privacy notice should include our lawful basis for processing as well as the purposes of the processing. (If our purposes change, we may be able to continue processing under

the original lawful basis if our new purpose is compatible with our initial purpose - unless our original lawful basis was consent).

Special Category Data

- While we may not regularly process special category data, there are instances where this might occur, such as when collecting diversity information during recruitment, retaining employee absence information or medical records, or carrying out DBS checks.
- In such cases, we need to identify both a lawful basis for general processing and an additional condition for processing this type of data. Special category data requires a higher level of protection, and processing it must be justified by both a lawful basis and an additional condition under the UK GDPR.
- Appropriate safeguards must be in place to ensure that this data is handled securely and in compliance with all relevant regulations.

For detailed guidelines, refer to Appendix 8: Fair processing procedure

Basic security

All staff are responsible for ensuring that any personal data they hold is kept securely and is not disclosed to any unauthorised third party. Personal data should only be accessible to those who need it for their work. Refer to our security policy in the policy section below for details on password security, the use of personal devices, and other relevant security measures.

Online and Computer security

We use cloud-based storage on OneDrive for electronically held data. All employees are required to set up 2-step verification for their Microsoft accounts to minimise the risk of unauthorised access. Failure to do so, or recklessly disclosing access codes, passwords, etc., may lead to disciplinary proceedings.

Key reminders:

- Install a firewall and virus-checking software on your computer.
- Ensure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates and installing anti-spyware software. McAfee offers this through our subscription.
- Do not share passwords.
- Encrypt any personal information held electronically that could cause damage or distress if it were lost or stolen.

- Never open spam emails.
- Carefully verify email addresses before sending messages to avoid unintended recipients. When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way – e.g. “Dave” - the auto-complete function may bring up several “Dave’s”. Make sure you choose the right address before you click send.
- Use blind carbon copy (bcc) instead of carbon copy (cc) when sending emails to groups to protect recipients' email addresses. When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- Be aware that if you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s arrangements are secure enough before sending your message.

Physical Security

Records such as our company book with the register of directors and meeting minutes, as well as any Gift Aid records in hard copy, bank statements, and others, are kept in our office under lock and key. These can only be accessed by those with a clear business need (currently CEO, Finance Manager, Governance Manager, and Finance Officer).

Our office itself is secured with locks and is located in an access-controlled building with a staffed reception. We believe we have taken appropriate security measures for physical data, considering the types of data we hold.

We have implemented a Clear Desk Policy to further enhance the security of physical data. This policy requires that:

- All employees must ensure that no sensitive documents are left out on desks when not in use. At the end of each working day, all documents containing personal or sensitive information must be securely stored in locked drawers or designated storage area.
- Computers and other electronic devices must be locked or logged off when unattended, even for short periods, to prevent unauthorised access.
- Any paperwork or notes that are no longer needed must be disposed of securely, using the shredders provided in the office.

- Personal items should be kept to a minimum on desks to avoid any confusion between personal and business-related documents.

Our policies

Security access policy

We have established specific requirements for protecting information and information systems against unauthorised access.

Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of WFSA which must be managed with care. All information has a value to the organisation. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

Definition

Access control rules and procedures are required to regulate who can access WFSA information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing WFSA information in any format, and on any device.

Scope

This policy applies to all WFSA 's Board and Council members, volunteers, stakeholders, partners, and employees (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the organisation with any form of access to WFSA's information and information systems.

Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may

intentionally or accidentally gain unauthorised access to business information which may adversely affect day-to-day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in a breach of data, financial loss and an inability to provide necessary services to our customers.

A Security Access Policy needs to be consistently enforced across the organisation. Inconsistent application of access controls, such as granting exceptions or overlooking access reviews, can create vulnerabilities and opportunities for unauthorised access.

Applying the Policy - Password Management

Choosing Passwords

Passwords are the first line of defence for our ICT systems and, together with the user ID, help establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact the confidentiality, integrity, or availability of our computers and systems.

Weak and Strong Passwords

- **Weak Passwords**: Easily discovered or detected, e.g., dictionary words, names, car registration numbers, simple keyboard patterns.
- **Strong Passwords**: Difficult to detect even with computer assistance, e.g., a mix of at least seven alpha and numeric characters, including special characters and avoiding easily guessable information like birthdays or names.

Password Standards

- At least seven characters.
- Contains a mix of alpha and numeric characters, with at least one digit.
- More complex than a single word.
- Includes special characters.

Protecting Passwords

To ensure passwords remain protected, adhere to the following guidelines:

- Never reveal your passwords to anyone.
- Never write down passwords or store them where they are vulnerable to theft.
- Store passwords in computer systems only with encryption.
- Avoid using any part of your username within the password.
- Use different passwords for different WFSA systems.
- Do not use the same password for work and external systems.

Changing Passwords

- Change all user-level passwords at least every 90 days or as prompted by the system.
- Immediately change default passwords and do not reuse them.
- Change passwords immediately if you suspect they are known to someone else and report this to the Finance Officer.

System Administration Standards

The password administration process for WFSA systems is well-documented and available to designated individuals. All WFSA IT systems will enforce the following:

- Individual user authentication, not group accounts.
- Protection for password retrieval and security details.
- User-level access monitoring and logging.
- Role management without password sharing.
- Controlled, secure, and auditable password administration processes.

Applying the Policy - User Access Control

Formal user access control procedures must be documented, implemented, and kept up to date for each application and information system to ensure authorised user access and prevent unauthorised access. These procedures must cover all stages of the user access lifecycle and be approved by WFSA.

Each user must have:

- Access rights and permissions commensurate with their tasks.
- A unique login not shared or disclosed to any other user.
- An associated unique password requested at each new login.
- Regular reviews of user access rights to ensure appropriate access.
- System administration accounts provided only to users required to perform system administration tasks.

User Registration

Requests for access to WFSA computer systems must be submitted to the Finance Officer. When an employee leaves, their access to systems and data must be suspended at the close of business on their last working day. The line manager must request this suspension from the Finance Officer.

User Responsibilities

Users must prevent unauthorised access by:

- Following the Password Policy Statements.
- Locking or logging out of unattended PCs.
- Not leaving access information, such as login names and passwords, on display.
- Informing the Finance Officer of any changes to their role and access requirements.

Applying the Policy - Remote Access Procedures

Network Access Control

Connecting USBs and using remote login methods on non-organisation owned PCs is not recommended. However, employees may use their WFSA login on non-WFSA laptops. All other network and device access policies remain in effect, and users are reminded to adhere to security protocols to protect organisational data.

User Authentication for External Connections

Requests for remote access to the WFSA network must be submitted to the Finance Officer and secured by two-factor authentication.

Supplier's Remote Access

Third-party suppliers must have CEO approval to access the WFSA network. Suppliers must contact the Finance Officer before connecting to the network, and a log of activity must be maintained. Remote access software must be disabled when not in use.

Operating System Access Control

Access to operating systems is controlled by a secure login process:

- No display of previous login information.
- Limiting unsuccessful attempts and locking accounts if exceeded.
- Hiding password characters by symbols.
- Displaying a general warning notice for authorised users only.
- Unique login IDs for auditing, not indicating access levels.
- Individual administrator accounts for system administrators, logged and audited.

Application and Information Access

Access within software applications must be restricted using the security features built into each product:

- Compliance with User Access Management and Password sections.

- Clearly defined roles.
- Appropriate access levels for user roles.
- Admin settings removed or hidden from users.
- Rights not overridden by operating system inheritance.
- Logged and auditable access.

Policy Compliance

If any user is found to have breached this policy, they may be subject to WFSA's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from Laurie Barnes or Kristine Stave immediately.

Privacy Policy

The WFSA privacy policy is reviewed annually to incorporate necessary changes due to evolving policies and legislation. The policy is accessible on our website via a link at the bottom of each page. It aims to outline our approach to privacy and protecting personal data in plain English.

The full text of our privacy policy is provided below. It is essential that all employees familiarise themselves with its contents, as it includes details on the retention periods of personal data for employees and volunteers.

Personal Information Collection

Visitors to Our Website
When visiting www.wfsahq.org, we use Google Analytics to collect standard internet log information and visitor behaviour patterns. This information helps us understand site usage without identifying individuals. If we intend to collect personally identifiable information, we will be transparent and explain its purpose.

We use WordPress, hosted by Cloudways, to publish our website and microsites. Google Analytics collects anonymous user activity data to monitor and improve site effectiveness. Visitors posting comments must provide a name and email address. For more information, refer to the Google Analytics privacy notice.

Links to Other Websites
Our website contains links to external websites. While we strive for accuracy, we cannot control external content. Our privacy policy applies only to our website. Please read the privacy policies of any external sites you visit.

Report faulty links to comms@wfsahq.org.

Contact

E-Newsletter

We use Mailchimp to deliver our e-newsletters, gathering statistics on email opens and clicks to improve our content. Refer to Mailchimp's privacy policy for more information.

Social Media Contact

The WFSA engages on LinkedIn, Facebook, and Twitter. Check each platform's privacy notice for details on personal data usage. Private messages sent to us via social media will remain on the respective platform and will not be shared with other organisations.

Email Contact

Emails sent to us are monitored for viruses and malware. Please ensure your emails comply with legal standards.

We retain personal details of those requesting our services to fulfil their requests. We may use this data for related purposes, such as feedback surveys. Subscribers to our services can cancel at any time through a simple process.

Recruitment and Employment

Job Applicants, Current, and Former Employees

The WFSA is the data controller for information provided during the recruitment process. Please see Appendix 6: Job applicant privacy notice. Contact us at admin@wfsahq.org for queries regarding data handling.

Successful applicants' information is retained for the duration of employment plus six years. Unsuccessful applicants' data is kept for six months post-campaign. Interview notes and other assessment data are also retained for six months. For information on employee data protection, please refer to Appendix 11: Employee Privacy Notice.

Volunteer Placements/Internships

Volunteers' applications are considered for suitability. If there are no current opportunities, we may retain applications for up to 12 months for future consideration with the applicant's consent.

WFSA Volunteer Privacy Notice:

This notice outlines how the WFSA collect, use, and protect your personal data.

1. Data Collection: WFSA collect personal information that you provide during your volunteer application and throughout your involvement with WFSA. This may include your name, contact details, and any other information necessary for your role.

2. Use of Data Your personal data is used to manage your volunteer role within WFSA, including communication, coordination of activities, and ensuring compliance with legal obligations.

3. Data Sharing WFSA may share your information with partners who assist us in managing/implementing our projects, but only as necessary and with appropriate safeguards in place. We do not sell or share your data with other organisations for marketing purposes.

4. Data Security WFSA take data security seriously and have implemented measures to protect your personal information from unauthorised access, disclosure, alteration, or destruction.

5. Your Rights You have the right to access, correct, or delete your personal data held by WFSA. If you wish to exercise any of these rights, please contact Laurie Barnes or Kristine Stave.

6. Data Retention We will retain your personal data only for as long as necessary to fulfil the purposes outlined in this notice or as required by law.

7. Contact Information For any questions or concerns regarding your personal data, please contact Laurie Barnes or Kristine Stave at WFSA.

Information Use and Retention
Information provided during recruitment is used solely to progress applications or meet legal requirements. We do not share this information for marketing purposes. Data is held securely in electronic or physical formats.

We contact applicants using the provided details to advance their applications and assess suitability for the role. We only collect necessary information and retain it no longer than required.

Data Processors
Third-party data processors help with recruitment services. They act only under our instructions, holding data securely and not sharing it with other organisations. Please see Appendix 7: Data processing by external suppliers' procedure

Moorepay
Employee details necessary for payroll services are provided to Moorepay, including salary, National Insurance number, date of birth, full name, and address.

Aviva
Employee details required for the pension scheme are provided to Aviva, including name, date of birth, National Insurance number, and salary. Bank details are not shared.

Your Rights
Individuals have rights regarding their personal data. For more information, visit the Information Commissioner's Office website: https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly.

Complaints or Queries
The WFSA strives to uphold high standards in data collection and use. Complaints are taken seriously. Suggestions for improvement are welcomed.

A detailed privacy notice is provided to all employees upon employment commencement and is included in the Staff Handbook. For UK regulatory information, visit the Information Commissioner's Office website: www.ico.org.uk.

Access to Personal Information
Individuals can request access to their personal data by submitting a written request to Laurie Barnes or Kristine Stave at the address below. Informal requests may be accommodated via telephone if agreed upon.

To correct any mistakes in the information we hold, contact Laurie Barnes or Kristine Stave.

Changes to This Privacy Notice
Our privacy notice is regularly reviewed and was last updated in June 2024.

Contact Information
For privacy policy inquiries, contact:
Laurie Barnes or Kristine Stave
WFSA
39-41, The Busworks,
North Road,
London N7 9DP,
United Kingdom

Cookies policy

This is also available online (at Privacy - WFSA (wfsahq.org) and sets out how we use cookies to optimise our website browsing experience:

What are cookies?

A cookie is a small piece of data or message that is sent from a website's server to your web browser and is then stored on your hard drive. They're generally used to improve your user experience by – for example – remembering what's in your online shopping basket or keeping you logged in on a website as you navigate from one page to another. Cookies can't read data off your hard drive or other cookie files, and do not damage your system.

Consent for cookies

The first time you access the website, you will be asked if you consent to receiving cookies. If you agree, cookies will be retained on your browser for that visit and for each time you subsequently access the website.

You also have an option not to use this feature, in which case no cookies will be retained on your browser. If you want to opt out of using cookies in future, then you can do so. It is important to note that if you change your settings and block cookies then our web site may not work so well. Your browser may be able to reject cookies, or to warn you before you download cookies, and information regarding this can be found in your browser's help facility.

How does WFSA use cookies?

- We use cookies so that you have a good experience when you visit our website.
- To remember your preferences such as language so that it is easier for you to navigate our website
- To track how visitors use our website so that we can improve and update our site
- To help manage your donation experience

Our website uses the following cookies:

Cookie name	**Purpose**
Functionality	WFSA uses these cookies so that we recognise you on our website and remember your previously selected preferences. These could include what language you prefer and your location. A mix of first-party and third-party cookies are used.

Data protection

Aim and Scope of Policy

This policy governs the processing of personal data within WFSA, covering both manual and electronic records in connection with its human resources functions. It also addresses responses to data breaches and other rights under the UK General Data Protection Regulation (UK-GDPR).

This policy applies to the personal data of job applicants, current and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors, collectively referred to as relevant individuals.

Definition

- **Personal Data**: Information related to an identifiable person, directly or indirectly, such as name, ID number, location, or online identifier, including pseudonymised data.
- **Special Categories of Personal Data**: Data related to health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, trade union membership, genetic and biometric data.
- **Criminal Offence Data**: Information related to criminal convictions and offences.
- **Data Processing**: Operations performed on personal data, such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, restriction, erasure, or destruction.

WFSA is committed to ensuring all personal data, including special categories and criminal offence data, is processed in line with the UK-GDPR and domestic laws. This commitment extends to all employees and third-party processors acting on behalf of WFSA.

Types of Data Held

Personal data is stored in personnel files or HR systems, including but not limited to:

- Contact information for individuals and next of kin
- CVs and recruitment information
- References from former employers
- National Insurance numbers
- Job titles, descriptions, and pay grades
- Conduct records and disciplinary proceedings
- Holiday records
- Performance information
- Medical and health information
- Sickness absence records
- Tax codes
- Employment terms and conditions
- Training details

Refer to the privacy notice for detailed information on processing activities, lawful bases for processing, and data retention periods.

Data Protection Principles

All personal data obtained and held by WFSA will:

- Be processed fairly, lawfully, and transparently with a valid legal basis.
- Be collected for specific, explicit, and legitimate purposes.
- Be adequate, relevant, and limited to what is necessary.
- Be kept accurate and up to date.
- Not be retained longer than necessary.
- Be processed securely to prevent unauthorised access, loss, or damage.
- Comply with GDPR procedures for international data transfers.

Personal data processing will respect individuals' rights, including the right to be informed, access, rectification, erasure, restriction, data portability, objection, and regulation of automated decision-making and profiling.

Procedures

WFSA has implemented procedures to protect personal data, including:

- Appointing employees with responsibilities for data processing, control, and auditing.
- Providing employees with information on data protection rights, usage, and protection measures.
- Offering training on data protection, confidentiality, and data breach actions.
- Accounting for all personal data sources and recipients.
- Conducting risk assessments to identify and mitigate data handling vulnerabilities. See Appendix 9: Privacy Impact Assessment
- Ensuring informed, specific, and unambiguous consent for data processing.
- Establishing mechanisms for detecting, reporting, and investigating data breaches.
- Complying with GDPR requirements for international data transfers.

Access to Data

Relevant individuals have the right to access their personal data held by WFSA. Access requests should be made using a form available from the Finance Officer. WFSA will respond to requests within one month, extendable by two months for complex requests. Inaccuracies in data will be promptly rectified. Please see Appendix 4

All requests should be recorded in the Data Subject Access Request Register. See Appendix 5: Register of Data Subject Access Requests.

Data Disclosures

Certain data disclosures may be necessary, including:

- Employee benefits operated by third parties.
- Reasonable adjustments for disabled individuals
- Health data for health and safety or occupational health obligations
- Statutory Sick Pay purposes
- HR management and administration
- Employee insurance policies or pension plans

Disclosures will be made only when necessary for the specific purpose.

Please see _Appendix_10:_Third Access to Data

Data Security

Security measures for storing and transporting data include:

- Securing confidential files and information
- Regular accuracy checks for data entry
- Using secure passwords and screen blanking
- Limiting the use of USB sticks and similar devices for personal data storage, using encryption when necessary

Non-compliance with data security measures may result in disciplinary actions, including dismissal.

International Data Transfers

WFSA does not routinely transfer personal data outside the UK. Any such transfer will comply with UK-GDPR requirements, ensuring adequate data protection levels or appropriate safeguards.

Breach Notification

WFSA has procedures to detect, report, and investigate data breaches. The ICO will be notified within 72 hours of a breach likely to risk individuals' rights and freedoms. Affected individuals will be informed without undue delay if the breach poses a high risk.

Training

All employees receive training on data protection, confidentiality, and data breach actions as part of their induction and through regular refresher sessions. Training records are maintained for compliance.

Records

WFSA maintains records of processing activities, including purposes and retention periods, in the HR Data Record, ensuring these records are up to date.

Data Protection Compliance

Laurie Barnes is the focal point for compliance on data protection activities within WFSA.

Security Incident Management

WFSA is committed to protecting its information assets from all threats, whether internal or external, deliberate or accidental. This procedure outlines the process for managing security incidents to minimise damage and ensure swift recovery, maintaining compliance with relevant data protection regulations.

Reporting Security Incidents

All suspected or actual security incidents must be reported immediately to Laurie Barnes, who is responsible for coordinating the response to security incidents. Please see Appendix 2: Security Incident Register.

Incident reports should include:

- A detailed description of the incident
- The time of occurrence
- Any initial actions taken

Incident Classification and Response

1. Confirm and classify the security incident.
2. Implement immediate measures to contain the incident and prevent further damage.
3. Identify and eliminate the root cause of the incident.
4. Restore affected systems and data to normal operation.
5. Conduct a post-incident review to identify improvements and prevent future incidents.

Incident Notification

During a security incident, regular updates must be provided to the CEO and relevant stakeholders. If necessary, communication with affected individuals, regulatory bodies, and the public must be handled in a transparent and legally compliant manner.

Record

WFSA is required to maintain comprehensive records of the incident, including response actions and decisions made. Laurie Barnes must document all communications and actions taken in response to the incident in the Internal Security Incident Register.

Data breach

The UK-GDPR states that there is a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data. We will need to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

WFSA has a data breach policy in place, as well as an internal data breach register. The formal data breach policy is copied below.

Scope

This procedure applies in the following events:

1. A personal data breach pursuant to Article 33 '*Notification of a personal data breach to the supervisory authority',* and

2. A personal data breach pursuant to Article 34 *'Communication of a personal data breach to the data subject'* of the UK-GDPR.

Data controller and data processor

There is a distinction under the UK-GDPR between a 'data controller' and a 'data processor'. This is because different organisations involved in processing personal data have varying degrees of responsibility. An organisation must choose whether it is a data controller or a data processor as regards a particular activity and cannot be both.

Responsibility

All users, including temporary employees of WFSA and third parties, must be aware of this procedure and are required to follow it should a personal data breach incident occur.

Procedure – Breach Notification

Data processor to data controller
All personal data breaches by WFSA must be notified to the appropriate data controller immediately. The person with responsibility for data protection in WFSA (currently Laurie Barnes)

must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided. Please refer to Appendix 3: Data incident report form.

Data controller to supervisory authority
All personal data breaches by WFSA must be notified to the appropriate supervisory authority immediately.

WFSA is required to carry out an assessment in order to determine whether the personal data breach is likely to cause a risk to the affected data subject's rights and freedoms under the UK-GDPR.

If a risk is considered likely, WFSA is required to report the personal data breach to the supervisory authority immediately and in any event, no later than 72 hours after the risk assessment. If the notification is made outside of the 72-hour window, WFSA is required to provide reasons for the delay.

Pursuant to External Breach Notification Record, WFSA is required to provide the following to the supervisory authority:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the CEO
- The likely outcomes of the personal data breach;
- Any measures taken by WFSA to address and/or mitigate the breach; and
- All other information regarding the data breach.

Laurie Barnes must record the communication of the breach in the Internal Personal Data Breach Register, stating how the notification was made (whether by email, telephone call etc.), to whom and how the confirmation of receipt was provided.

Data controller to data subject
If it is likely that there will be a high risk to the affected data subject's rights and freedoms under the UK-GDPR, WFSA is required to provide immediate notification to the relevant data subjects.

The notification to the data subject must be made in clear and plain language and must include the following:

- A description of the nature of the personal data breach;
- The categories of personal data that have been affected by the breach;
- The number, which may be approximated if necessary, of data subjects affected by the breach;
- The number, which may be approximated if necessary, of personal data records affected by the breach;
- The name and contact details of the CEO;
- The likely outcomes of the personal data breach;
- Any measures taken by WFSA to address and/or mitigate the breach; and
- All other information regarding the data breach.

WFSA must use appropriate measures, such as encryption, to ensure that all personal data is secure and cannot be accessed by those without the requisite authority. WFSA must also take subsequent measures to ensure that the risk to the rights and freedoms of the data subject are no longer an issue.

If notification would require the WFSA to implement a disproportionate amount of effort, a public communication or other similar measure may suffice, as long as all data subjects are effectively informed. It is possible that the supervisory authority may require WFSA to communicate the personal data breach to the data subject, should there be an element of high risk involved.

Record-keeping

Record keeping is an important but often overlooked part of running or working in a voluntary organisation. It is vital for good governance and necessary for complying with the wide range of regulations that apply to charities all around the world.

Good record keeping will:

- Show that we are complying with relevant regulations.
- Provide evidence of how we have made decisions and demonstrate good governance and processes.
- Make day-to-day work more efficient as staff members, trustees and volunteers know where to find information.
- Make it easier to show the impact of our organisation.

- Build trust with donors, funders, regulators and the public as they know that organisations can provide evidence and be held accountable for their actions and decisions.

What are 'records'?

Records are the documents which are generated by the work of the organisation. Records may include but are not limited to documents, files, electronic records, emails, correspondence, financial records, contracts, personnel records, and personal data. These documents can be current, used for the current day-to-day running of the organisation. They can also be historical, showing how an organisation made decisions in the past. Not every document should be retained for permanent preservation, but those that are preserved are commonly known as archives. Collectively, records should reflect the work of an organisation. They might be organised by the functions or activities of different departments and directorates, but overall they should tell anyone who consults them, who we are, how we are run and what we do.

Records shall be organised and classified in a logical and consistent manner to facilitate retrieval and ensure efficient access. Access to records shall be granted on a need-to-know basis, with appropriate security measures in place to protect sensitive or confidential information.

Responsibility

Board members: As persons with the overall legal responsibility for ensuring that a charity is well-run, trustees play a vital role in ensuring that the organisation is a responsible record-keeper. Principle six of the UK's 'Good Governance: A Code for the Voluntary Sector' (2010, Second Edition) explicitly states that this is the responsibility of trustees to provide good governance and leadership through: "complying with any applicable legal or regulatory requirements concerning records". The Charity Commission expects trustees to be responsible for complying with these regulations, and has statutory powers allowing them to intervene where trustees fail to perform this role. While WFSA is not governed by Charity Commission guidelines, it is prudent to adopt these given that our headquarters are based in the United Kingdom.

Senior management: Trustees are supported in their role by other executives and those in senior management, through their delegated powers to oversee the work of the charity, both on a day-to-day and longer-term basis. This includes records management and sits alongside any powers they may hold or responsibilities they have to ensure regulatory compliance.

Staff: Staff are responsible for ensuring that the correct records management policies and procedures are followed, as well as training and supervising volunteers in records management best practice.

Volunteers: Volunteers need to ensure that they create and store records in accordance with the organisation's records management policy.

Retention policy

We have updated our records retention policy in light of the UK-GDPR and made this available to all staff as part of the employee handbook.

The most important thing to note is that the periods for which records need to be kept depend on what they are, what their historical value might be, our business need and of course the rules and regulations governing the specific types of records.

We will always pay proper attention to the provisions of the relevant regulations and never keep personal details for longer than required.

Below is a list of the different types of records WFSA (UK) keeps and detail of how long each of these must be kept:

Record description	***Retention period***	***Comments***
Registers, founding documents and Charities Act (CA) records		
Register of directors	Life of charity (CA s.162)	
Register of secretaries	Life of charity (CA s. 275)	
Directors' residential addresses	Life of charity (CA s.165)	
Register of charges	Life of charity (CA s.876)	
Register of members	Life of charity (CA ss.113-121)	
Articles of association	Life of charity	
Certificate of incorporation	Life of charity	
Copies of resolutions filed at Companies House	While resolution or agreement is in force (CA s.29)	

Register of trustees' declarations of interest	At least 10 years	
Statutory returns		
Annual returns to Companies House (CH)	3 years	Access through online CH system
Forms regarding directors and secretaries appointments		Hard copies printed out and signed
Copies of other statutory returns filed with CH or Charity Commission		Access through CH/CC online systems
Board meetings		
Agenda papers	7 years	
Board minutes	10 years from date of meeting (CA s.248)	Printed out and signed by Secretary upon confirmation of accuracy
Written resolutions of the Board	10 years from date of meeting (CA s.248)	Printed out and signed by trustees
Board committee minutes	10 years from date of meeting (CA s.248)	Printed out and signed by Secretary upon confirmation of accuracy
Agreements and related correspondence		
Contracts with customers, suppliers or agents	6 years after expiry or termination of contract	6 years is generally the time limit within which proceedings based on a contract can be brought in the UK (Limitations Act 1980)
Licensing agreements		
Rental/hire purchase agreements		
Indemnities and guarantees		
Others		

agreements/contracts		
Property		
Deeds of title	Permanently or until property is disposed of	
Leases	15 years after expiry (Limitations Act 1960)	
Records of major refurbishments, warranties, planning consents, design documents, final health and safety files	13 years for actions against contractors etc.(Data Protection Act)	
Accounts		
Company accounts and accounting records	6 years from the date they are made (Charities Act 2011, s.131)	
Annual reports and accounts (signed)	6 years (VAT Act 1994, sch.11)	
Tax and payroll		
VAT records	6 years	If there is a tax enquiry ongoing, records should be retained until the enquiry is complete
PAYE	Minimum 3 years after the end of the tax year to which they relate (Income Tax (PAYE) Regulations 2003, reg.97)	
Notice to employer of tax code (P6)	6 years plus current year (Taxes Management Act)	
Certificate of pay and tax deducted (P60)		

Income tax records re employees leaving i.e. P45		
Annual return of employees and directors expenses and benefits (P11D)		
Annual return of taxable pay and tax deducted		
Records of pension deductions (including superannuation)	6 years plus current year (Pensions Act)	
Banking records		
Bank paying-in books	6 years (CA, s.388)	
Bank statements		
Remittance advices		
Bank reconciliations		
Sales ledger/receipt cash book	10 years (Companies Act/Charities Act and HMRC)	
Insurance documents		
Policies	3 years after lapse (Data Protection Act)	
Claims correspondent	3 years after settlement (Data Protection Act)	
Employers Liability insurance Certificate	40 years (Employers' Liability (Comp. Insurance) Regulations 1998)	
Accident reports and relevant correspondence	3 years after settlement (Data Protection Act)	
Organisation charts	Life of charity	
Personnel files and training records	6 years after employment ceases (Limitations Act	Records for senior management will be kept

	1980)	permanently for historical purposes
Wage and salary records	6 years plus the current year (Taxes Management Act)	
Expense accounts records		
Overtime/TOIL records		
Applications forms/interview notes (for unsuccessful candidates)	6- months	Disability Discrimination Act 2009 and Race Relations Act 1976 recommend 6 months. One year limitation for defamation actions under Limitations Act
Redundancy details, calculations of payments, refunds, notifications to the Secretary of State	6 years from the date of redundancy.	
Statutory Maternity Pay records, calculations, certificates or other medical evidence	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.	
Statutory Sick Pay records, calculations, certificates, self-certificates	Six years after employment ends	There is no longer a specific statutory retention period but for business need we keep records for 6 years after employment has ended
Donor/customer records		
Correspondence about donations	6 years from the end of the financial year in which the transaction was made.	
Gift Aid declarations	6 years after the last payment made (Data Protection Act)	
Legacies	6 years after the estate has been wound up (Data Protection Act)	

Correspondence with customers/beneficiaries	2 years after the date of receipt of goods (Data Protection Act)	Product warranty also expires after 2 years

In addition, health and safety records will be kept as required by the 1974 Health and Safety at Work Act:

- Reportable Injuries, disease and dangerous occurrences (3 years)
- Accident book (3 years from the last entry)

Direct marketing

What is meant by direct marketing?

Direct marketing is defined as 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals'. This definition covers any advertising or marketing material, not just commercial marketing. All promotional material falls within this definition, including material promoting the aims and ideals of not-for-profit organisations such as WFSA. We must in particular be mindful that the definition of direct marketing will cover any messages that contain marketing elements even if this is not the main purpose of the message.

If an organisation is sending unsolicited direct marketing by electronic means, or employing someone else to do so on its behalf, it must comply with PECR (see above). This includes telephone calls (both live and automated), faxes, emails, text messages and other forms of electronic message.

To be clear: Legally, direct marketing means directing any advertising or marketing material to particular individuals. The ICO has issued guidance stating that 'advertising or marketing material' includes any material which promotes the aims and objectives of the organisation, not just about promoting products or services. In other words, as we are a charity and using supporters' contact details to keep in touch with them about fundraising campaigns or news about our work, we are doing direct marketing.

Consent for direct marketing

We must be able to demonstrate that consent was knowingly and freely given, clear and specific. We must keep clear records of consent so we can demonstrate compliance in the event of a complaint (going forward, this will be done on the data subject's record on Salesforce): We will record the date of consent, the method of consent, who obtained consent, and exactly what information was provided to the person consenting.

If someone claims that they did not consent to receive our marketing messages such as the e-newsletter, we may be at risk of enforcement action unless we can demonstrate that the person did in fact give valid consent.

The ICO recommends that consent be provided through a clear and affirmative action, such as ticking a checkbox, signing a consent form, or actively opting in. It should not be assumed from silence or inactivity.

The rules on calls, texts and emails are stricter than those on mail marketing, and consent must be more specific: We cannot take a one-size-fits-all approach to this.

Consent requests for direct marketing should be separate from other terms and conditions, ensuring that individuals can easily understand and provide specific consent for marketing purposes without any confusion.

> ***Example:***
> An individual sees our appeal in a medical journal and decides to donate £5 by text message. However the fact that the individual has decided to donate on this occasion (and provided their number to us as a result) does not mean that we have their consent to use their details to contact them about future campaigns. We cannot therefore use the individual's details for marketing purposes. The same would be true if the individual gave through email or an online site which provided us with their email address.

Consent does not last forever. It is good practice to renew consent every two years. (Consent under PECR is expressly considered to be 'for the time being'. The ICO considers that this implies a period of continuity and stability, and that any significant change in circumstances is likely to mean that consent comes to an end.)

We must carry out rigorous checks before relying on indirect consent (i.e. consent originally given to a third party). Indirect consent is highly unlikely to be valid for calls, texts or emails. While the use of marketing lists are now banned, we must take steps to ensure a list was compiled fairly and accurately reflects peoples' wishes. Bought-in call lists should be screened against the Telephone Preference Service (TPS). It will clearly be very difficult to use bought-in lists for text, email, or automated call campaigns as these require very specific consent (either where WFSA is named or it is within a precisely defined category of organisation).

(A 'soft opt-in' exception applies to commercial marketing of products or services only. While nonprofits might be able to use the soft opt-in for any commercial products or services they offer,

we cannot send campaigning texts or emails without specific consent, even to existing supporters.)

Opting out

We must stop sending marketing messages to any person who objects or opts out of receiving them. (The ICO will consider using its enforcement powers, including the power to issue a fine of up to £500,000, where an organisation persistently ignores individuals' objections to marketing or otherwise fails to comply with the law).

We must not make it difficult to opt out, for example by asking someone to complete a form or confirm in writing. In any event, as soon as a customer has clearly said that they don't want the texts or emails, we must stop, even if the customer hasn't used its preferred method of communication.

Marketing calls

We can make live marketing calls to numbers not registered with the Telephone Preference Service (TPS), if it is fair to do so. We must not call any number on the TPS list without specific prior consent. We must not make any automated pre-recorded marketing calls without specific prior consent. Organisations making marketing calls must allow their number (or an alternative contact number) to be displayed to the person receiving the call.

Exception for market research

The direct marketing rules will not apply if we contact customers to conduct genuine market research (for example the purpose is to use market research to make decisions for commercial or public policy) or contracts a research firm to do so, as this will not involve the communication of advertising or marketing material.

However, we cannot avoid the direct marketing rules by labelling our message as a survey or market research if it is actually trying to sell goods or services, or to collect data to help us (or others) to contact people for marketing purposes at a later date. This is sometimes referred to as 'sugging' (selling under the guise of research). If the call or message includes any promotional material, or collects data to use in future marketing exercises, the call or message will be for direct marketing purposes. The organisation must say so and comply with the UK GDPR and PECR direct marketing rules.

Solicited versus unsolicited marketing

There is no restriction on sending solicited marketing – that is, marketing material that the person has specifically requested. PECR rules only apply to 'unsolicited' marketing messages, and the UK

GDPR will not prevent us providing information which someone has asked for. So, if someone specifically asks us to send them particular marketing material, we can do so.

If the marketing has not been specifically requested, it will be unsolicited and the PECR rules apply. This is true even if the customer has 'opted in' to receiving marketing from us.

Suppression list

We need to maintain a 'suppression list' of people who have opted out or otherwise told us directly that they do not want to receive marketing. (Individuals may ask us to remove or delete their details from a database or marketing list. However, in most cases we should instead follow the marketing industry practice of suppressing their details.) Rather than deleting an individual's details entirely, suppression involves retaining just enough information to ensure that their preferences are respected in the future.

Suppression allows us to ensure that we do not send marketing to people who have previously asked us not to, as there is a record against which to screen any new marketing lists. If people's details are deleted entirely, there is no way of ensuring that they are not put back on our database. Deleting details might also breach industry-specific legal requirements about how long to hold personal data.

We must not contact people on a suppression list at a later date to ask them if they want to opt back in to receiving marketing. This contact would involve using their personal data for direct marketing purposes and is likely to breach the UK-GDPR and will also breach PECR if the contact is by phone, text or email.

However, people can of course change their minds and marketing strategies also change. There is some merit in making sure that the information about people's preferences is accurate and up to date. The ICO considers that it can be acceptable to send a message immediately after someone has opted out confirming they have unsubscribed and providing information about how to resubscribe, or to remind individuals that they can opt back in to marketing if the reminder forms a minor and incidental addition to a message being sent anyway for another purpose. However, we must do this sensitively, must not include marketing material in the message, and must never require an individual to take action to confirm their opt-out.

More information is available on the ICO website: https://ico.org.uk/for-organisations/guidance-index

Other resources

- Institute of Fundraising Code of Practice: https://www.youtube.com/watch?v=eem_JkxKYdY
- ICO direct marketing guidance for charities webinar: https://www.youtube.com/watch?v=WqlRVx_vae0&t=1643s
- ICO subject access requests webinar: https://youtu.be/ygGnxIYCOcI?list=PLaprDSeyZ5_6-BybH0enoXd4QlWXqsGc9

Step-by-step

Understanding the purposes of the UK-GDPR

The UK-GDPR legislation is there to protect individuals. The processing of their personal data is strictly limited and normally will require their consent. The UK-GDPR is designed to put control of a person's personal information very much in the hands of the data subject. They will decide how long we can keep it, what we do with it and with whom we share it.

They have many rights including the right to be forgotten or erased, the right to restrict the processing of data and most importantly, the right to object to the processing of their data. Our understanding of the principles of data protection will underpin policies and procedures in the future.

What is a data controller?

Data controllers collect, retain, own and erase the data. They also pass it to the data processors for processing. Data Controllers have to be clear on the purpose of collecting and processing the data. Consent should be obtained from data subjects by the Data Controller.

What is a data processor?

If you are acting under the instruction of a data controller to perform a task with data supplied to you by them, then you are only processing the data or performing a task on behalf of the controller. The best example is your print company who might be printing personalised letters or invites to an event. The printer in this example is merely using the data for the purpose instructed, they have no control or responsibility for the data other than that task. The processor adopts no responsibility for the data other than to excuse the given task in hand. The Controller is responsible for choosing the processor and ensuring that they are suitable to undertake the task. The processor should have adequate data protection policies no more onerous than the controller.

What is meant by processing data?

The processing of data includes, collecting data, storing data, communicating with data subjects (individuals) by whichever channel and condition (online, on the phone, SMS, apps, emails and etc.), sharing data with a third party and deleting data.

What is meant by categories of data?

A category refers to a type of personal data. For example, one category could be a person's name, another could be their postal address, and another could be their email address. It is important that we detail which categories of data we are collecting and understand precisely the reasons for collecting this data.

While we generally do not collect special category data (such as religion, gender, sexual orientation, or individual health data) that requires an enhanced level of consent to process, there are exceptions. For instance, during recruitment, we may collect special category data if an applicant discloses a disability, as this is necessary to comply with our obligations under the Equality Act 2010.

When processing such data, we must ensure that we have both a lawful basis for processing and meet an additional condition for processing special category data under the UK GDPR. This ensures that the data is handled with the necessary level of protection.

Appointing a DPO

We do not need to appoint a DPO as we are not processing 'Special categories' of data. Laurie Barnes has taken on the role as the organisational lead for data protection.

Guidelines on Data Protection and Privacy Policies

What information do we need to provide to data subjects on how their personal data will be used?

- The name of the data controller and how to contact them.
- The name of organisational lead for data protection (currently Laurie Barnes).
- The purpose we are collecting the data, i.e., marketing
- Whether we intend to transfer their data outside of the UK
- An explanation of our data retention policy and therefore how long we intend to keep their data
- Our Legitimate Interest.
- The subject's right to data accuracy and data rectification
- Their right to withdraw consent should they have given it. This will include Opt-out in some cases
- Their right to complain about us to the ICO and how to contact the ICO
- Whether we intend to profile their data and the ability to Opt-out of this if they so wish.
- If we have received the data from a third party, we must tell the subject about this, where we obtained the information and how we keep data secure.

Note: This is all contained in our privacy policy displayed on the website.

Requirement to keep information up-to-date and accurate

The fourth principle of the UK GDPR demands that you keep data up to date. We cannot entirely rely on the data subject to do this. Royal Mail has a service called NCOA that can assist with this but it remains our responsibility to keep data up to date.

Keeping data only for the purpose for which it was collected

This is very important. If we collected the data for a specific reason such as an event, we cannot process it for another reason unless we told the data subject at the point of collection. We need to be specific in our privacy notices; when you communicate with stakeholders and contacts you must be clear, transparent and honest about what we are doing.

Keeping data for a legal or regulatory reason

Having set our data retention policy as above, we will be regularly deleting data in the future. However, even if a data subject requests to be forgotten we may need to keep the data. This will be because we may have a legal claim against us in the future. Therefore, we will need to find a way of suppressing our database to keep the data for up to six years but not process it for another reason such as marketing. We will regularly review the data retention period of such data to ensure we are not keeping it for any longer than is necessary.

About data subject rights

Data subjects can request that we give them all the data we hold about them in any format; including hard copies, electronic and media files.

We have a Data Subject Access Request policy which individuals can follow to obtain copies of their data hold. Under the ICO guidelines, organisations should be able to respond to DSARs within one month and must keep all the information in a manner that is easily accessible when requested.

Conditions for processing data

For processing to be lawful under the UK GDPR, we need to identify a lawful basis before we can process personal data. These are often referred to as the “conditions for processing” under the DPA 1998. It is important that we determine your lawful basis for processing personal data and document this. This becomes more of an issue under the UK GDPR because our lawful basis for processing has an effect on individuals’ rights. For example, if we rely on someone’s consent to process their data, they will generally have stronger rights, for example to have their data deleted.

WFSA processes data based on the pursuit of legitimate interests, meeting contractual obligations, legal obligations and consent.

We obtain specific consent for email communications - see section above about direct marketing. This must be recorded on the data subject's electronic record with the date when consent was given.

International transfers of data

The UK-GDPR imposes restrictions on the transfer of personal data outside the UK, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the UK-GDPR is not undermined.

The UK and EU currently have an adequacy agreement in place on data protection. The EU-U.S Data Privacy Framework (EU-U.S DPF) and the UK Extension to the EU-U.S. DPF facilitate personal data transfers from the EU and the UK to the U.S. The EU-U.S DPF became effective on 10 July 2023, allowing the transfer of EU personal data to compliant U.S organisations. The UK Extension to the EU-U.S DPF took effect on 12 October 2023, permitting transfers from the UK. Care must be taken with U.S based data processors. Ensure they participate in the relevant Data Privacy Frameworks and are listed on the Data Privacy Framework List to confirm compliance.

Transferring data to a country outside the UK requires an adequacy provision to be in place. This means that the level of data protection is at least as robust as the provisions of the UK-GDPR. The ICO can help with identifying if a country is covered.

Children's personal data

We do not process personal data on children. The section below is for general information only.

The UK-GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand. If you offer an 'information society service' (i.e. online service) to children, you may need to obtain consent from a parent or guardian to process the child's data.

The UK GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility'. But note that it does permit for a lower age in law, as long as it is not below 13. 'Information society services' includes most internet services provided at the user's request, normally for remuneration. The UK-GDPR emphasises that protection is

particularly significant where children's personal information is used for the purposes of marketing and creating online profiles. Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

Wealth screening

Wealth screening should not be done without giving donors an explicit, detailed explanation of how we plan to use their data. We must notify people of plans to use their data even if it comes from publicly available sources. This is done in our privacy policy published online.

If we at any time decide to use a third party to carry out wealth screening, separate consent will be needed to share the data with every single third-party organisation. We will need to have a data contract with third parties to uphold the rights of data subjects and to protect the interests of WFSA and ensure secure transfer of data across in its journey for wealth screening.

Guidelines on using photographs

You should obtain the subject's consent in writing before photographing; this is the easiest and safest way of proving you have obtained the image fairly and in accordance with the individual's rights, both key elements of DPA (Data Protection Act) compliance.

To get this consent, ensure you obtain an image release form. This ensures that when you collect the image(s) you are not only acquiring consent, but also telling the subject what is being collected, why it is being collected and the limits on processing (use, disclosure and disposal).

You should ensure the following is covered in the form:

- a statement that WFSA processes and stores information in accordance with the Data Protection Act (DPA) 1998 / the UK General Data Protection Regulation (UK-GDPR)
- an explanation of the main reason for collecting the image, the purpose of processing
- a means of obtaining the consent of the individual where required, for example, when intending to publish their image or when taking it from or passing it to third parties
- whether the image will be released to third parties and who those third parties are
- where the image will be used
- a means for the individual to opt out now or later if they wish
- how long the image will be held, how it will be maintained and eventually destroyed
- an explanation of how the individual can see the personal information about them being held

Photographs of large groups

It will usually be enough for the photographer to verbally ask permission to take the photograph to ensure compliance with the DPA. Anyone not wishing to appear on a group photograph will then have the opportunity to opt out. This approach can be used when photographing, for instance, a seminar.

Photographs of small groups

For photographs taken of a small group of individuals best practice would be to seek consent before photographing begins. When acquiring this consent, it is important to ensure that individuals are informed what the images will be used for (for example where they will be published and who will have access to them).

In most cases, verbal consent is all that will be required although photographers may wish to use the standard image release form to be signed by the subject(s), to ensure that they have appropriate consent.

Photographs on the web

If you wish to use photographs of individuals on a website, the information is potentially being disclosed beyond the UK and, consequently, it is essential that the explicit consent of the individuals concerned is obtained. You can use the standard image release form to obtain this consent.

When displaying/disclosing personal information in either of these ways, you have a duty, under the UK GDPR, to keep the information up to date. Also, you must provide the employees with a means of opting out at a later stage even if initially they gave their consent.

Photographs and sensitive personal data

The legislation defines sensitive personal data as a class of data with special rights. This data can only be used in appropriate circumstances, such as a medical context or in the pursuit of equal opportunities.

If you suspect the images you are about to process could be sensitive personal data, please contact Laurie Barnes for guidance.

Exemptions from the Data Protection Act

The legislation provides some exemptions from the Act's provisions if, for instance, images are being processed for journalistic, literary and artistic purposes, or for research purposes. It is difficult to provide generic guidance here as each case must be dealt with on a case-by-case basis.

If you believe the images you are processing could fit these exemptions, please contact Laurie Barnes for guidance.

Using images without the consent of the subject

Using images of people who have not given their consent can expose WFSA to the risk of a legal claim or damage of reputation. If you do not have the consent of the subject, then consider using a different (more reliable) image.

If you suspect the images you are about to process are without the consent of subjects, please contact Laurie Barnes for guidance.

Storage of photographic images

Under the legislation photographs (as personal data) must be kept secure.

Checklist when processing photographic images

Some questions to consider when processing photographic images:

- For what purpose was the photograph originally taken? Bear in mind that if it was taken for one purpose (for example, personal use) it cannot then be used for another (for example, business use) without the explicit consent of the individuals concerned
- Is the image sensitive personal data? If it is, do you have the data subject's explicit consent?
- When photographing with small groups and individuals, has an image release form been used*?*
- When photographing large groups, have the individuals been given a chance to opt out of the photograph?
- Has the subject been told how the image will be used?
- Are you using the image according to how the subject was told it would be used?
- Are you authorised to process the image?
- Has the person with responsibility for data protection in WFSA been notified that you are processing images for a particular purpose?
- Are you sure that the image will be held securely?
- If you do not have the subject's consent to process their image, what is the purpose of this image?
- Do you know how long to keep the image for, and when and how to dispose of it?

Compliance

Registering with the ICO

As WFSA was established for not-for-profit making purposes and we do not make a profit (or only make a profit for our own purposes) we are not required to register with the ICO.

Employee training

Organisations are required to evidence their compliance with the UK-GDPR and the recording and monitoring of employee training will be a vital aspect of evidencing this. Whilst a certain element of employee training has to be generic around the UK-GDPR, it also needs to be specific to the organisation concerned. Employees should be able to relate the policies and procedures the organisation has in place around the UK-GDPR compliance, to their day-to-day roles when they handle and deal with data as part of their daily working life.

WFSA's training policy

WFSA is responsible for ensuring that all employees who are responsible, on a day-to-day basis, for compliance with the UK GDPR and relevant good practice, are able to exhibit competency in their understanding of the UK-GDPR, good practice and the implementation thereof by WFSA.

All persons with the UK-GDPR responsibility shall receive appropriate training and all training records are to be maintained by the Governance Assistant.

WFSA shall also be responsible for ensuring that all persons with the UK-GDPR responsibility are regularly informed of and updated on all relevant matters related to personal data management, including through contact with external bodies, the most noteworthy of which is the Information Commissioner's Office (www.ico.gov.uk). WFSA shall keep a list of all relevant external bodies for reference at all times.

WFSA is responsible for ensuring that all of its employees are aware of their personal responsibilities in relation to personal data, ensuring that it is properly protected at all times and is processed only in line with WFSA's procedures. To this end, WFSA shall ensure that all of its employees are given appropriate and relevant training. Laurie Barnes will organise both specific training for the UK-GDPR responsible persons as well as general training for all staff and to maintain records of completion.

Appendices

Appendix 1: Employee acknowledgement

Employee acknowledgement of UK-GDPR Principles and WFSA's implementation

I, the undersigned, hereby agree that at all times, whether or not in the employ of WFSA, and except where such information is in the public domain, I will:

- Maintain confidentiality with regards to the business affairs of the organisation, its customers, products, and product lists strictly confidential. I will only disclose such information if authorised by the board of directors, a court of law, an authorised enforcement agency (e.g., police, regulatory bodies under the Financial Services Act, HM Revenue & Customs), or as required by public interest disclosure legislation.
- Protect confidential information by refraining from revealing or using confidential information regarding systems, programme design, and data for personal gain.
- Use computer equipment and access the internet only when authorised to do so and solely for official employer business. I understand that unauthorised usage could result in damage to equipment and loss of stored data.

I commit to familiarising myself with the data protection procedures established by WFSA in compliance with the UK General Data Protection Regulation (UK-GDPR). I understand that the organisation must treat any breach of these procedures as a serious disciplinary matter.

I acknowledge that any breach of this agreement could lead to the disclosure of the organisation's sensitive and confidential data to competitors or other interested parties. I am aware that such conduct may result in summary dismissal under the disciplinary procedure.

Date:

Name of Employee:

Signature:

Appendix 2: Security Incident Register

Security Incident Register (sharepoint.com)

- Incident ID: A unique identifier for each incident.
- Date & Time Reported: When the incident was reported.
- Reported By: Name of the person reporting the incident.
- Description of Incident: A brief summary of what happened.
- Date & Time of Incident: When the incident occurred.
- Location: Where the incident took place.
- Type of Incident: Classification of the incident (e.g., data breach, unauthorised access).
- Initial Actions Taken: Immediate measures implemented to contain the incident.
- Responsible Person: The individual responsible for managing the incident response.
- Status: Current status of the incident (e.g., ongoing, resolved).
- Actions Taken: Steps taken to address and mitigate the incident.
- Root Cause: The underlying cause of the incident.
- Preventive Measures: Actions taken to prevent a recurrence.
- Date Closed: When the incident was resolved.
- Notes: Additional relevant information.

Appendix 3: Data incident report form

	Report prepared by: **Date:** **On behalf of:**	Name Date Organisation
1	**Notification**	How the notification was made: email, telephone etc. To whom: please indicate who the incident was notified to
2	**Summary of the event and circumstances**	When (date and time), what (Any relevant context or background information.), who (describe how the incident occurred, including any relevant technical details, vulnerabilities, or contributing factors).
3	**Type of Incident: Select the appropriate option**	- Unauthorised access or disclosure of personal data - Loss or theft of data storage devices - Data breach due to cyber-attack or hacking - Accidental or inadvertent disclosure of personal data - Other (please specify)
4	**Title or name of the document/s: What personal information is included**	Name; Address; DoB; Bank account details; description of information about an individual (health issues; notes/decisions etc.)
5	**Amount of personal data**	Specify the number or estimated number of individuals affected by the incident, if known.
6	**Severity of Incident: Select the appropriate option**	- Low: Minimal or no impact on individuals' rights and freedoms - Medium: Moderate impact on individuals' rights and freedoms - High: Significant impact on individuals' rights and freedoms

7	**Actions taken by recipient when they inadvertently received the information**	Describe the initial steps or actions taken to address the incident immediately after its discovery.
8	**Actions taken to retrieve information and respond to the breach**	Has information been retrieved? When? Has loss been contained? e.g. all emails deleted
9	**Procedures / instructions in place to minimise risks to security data**	(communication, secure storage, sharing and exchange)
10	**Breach of procedure/policy by staff member**	Has there been a breach of policy? Has appropriate management action been taken?
11	**Details of notification to the affected data subject**	Has the data subject been notified? If not, explain why not? What advice has been given to the affected data subjects?
12	**Details of data protection training provided**	Include date of last training prior to the incident by the staff member breaching security
13	**Procedure changes to reduce risks of future data loss**	
14	**Conclusion**	Serious/minor breach, likelihood of happening again

Appendix 4: Data Subject Access Request form

1. Data Subject Details

Title: Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Other ☐
Surname:
First Name(s):
Current Address:
Telephone Number
Home:
Work:
Mobile:
Email Address:
Date of Birth:
Documents Provided for Identity Verification ☐ Passport ☐ Driving License ☐ National ID Card ☐ Other (Please specify):
Are you acting on behalf of the data subject with their written or other legal authority? Yes ☐ No ☐
If 'Yes', please state your relationship with the data subject (e.g. parent, legal guardian, solicitor):
Please enclose proof that you are legally authorised to obtain this information.
2. Details of Person Requesting the Information
Date of Request:
Type of Request: ☐ Access to Personal Data ☐ Rectification of Data ☐ Erasure of Data (Right to be Forgotten) ☐ Restriction of Processing ☐ Data Portability

☐ Objection to Processing ☐ Other (Please specify):
Description of Request:
Section 3: Response to Request
Data Provided: ☐Yes ☐ No (If No, state reason):
Date Data Provided:
Format of Data Provided: ☐ Electronic Copy ☐ Physical Copy
Section 4: Additional Comments
Notes:

Declaration

I, ..., the signatory and person identified above as the data subject, hereby request that WFSA provide me with the personal data about me identified above.

Signature: _____

Date: _____

DSAR form completed by: [Insert employee name]

Please note: This form must be immediately forwarded to the WFSA CEO.

Appendix 5: Register of Data Subject Access Requests

Excel saved on One Drive

- Date request received:
- Request Description:
- Request Type:
  [Specify the type of request made by the individual, such as access to personal data, rectification, erasure, restriction of processing, data portability, or objection to processing.]
- Identifying number:
- Identity Verification:
- Yes/No
- Original deadline for:
- Extended deadline for:
- Date employee advised:
- Date response:
- Were subject access rights restricted?
- Yes/No
- Follow up action:

Appendix 6: Job applicant privacy notice

WFSA: Job Applicant Privacy Notice

As part of any recruitment process, WFSA collects and processes personal data relating to job applicants. WFSA is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does WFSA collect?

WFSA collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

WFSA may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

WFSA may also collect personal data about you from third parties, such as references supplied by former employers.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does WFSA process personal data?

WFSA needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, WFSA needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

WFSA has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The WFSA may also need to process data from job applicants to respond to and defend against legal claims.

WFSA may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. It may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who

have a disability. The organisation processes such information to carry out its obligations and exercise specific rights in relation to employment.

If your application is unsuccessful, WFSA may keep your personal data on file in case there are future employment opportunities for which you may be suited. The organisation will ask for your consent before it keeps your data for this purpose and you are free to withdraw your consent at any time.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the operational team and recruiting managers, interviewers involved in the recruitment process and managers in the business area with a vacancy.

WFSA will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The organisation will then share your data with former employers to obtain references for you.

The organisation will not transfer your data outside the UK.

How does WFSA protect data?

WFSA takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

For how long does the organisation keep data?

If your application for employment is unsuccessful, the organisation will hold your data on file for 6 months after the end of the relevant recruitment process. At the end of that period your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Laurie Barnes at laurie.barnes@wfsahq.org.

If you believe that the WFSA has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to WFSA during the recruitment process. However, if you do not provide the information, the organisation may not be able to process your application properly or at all.

Automated decision-making

Recruitment processes are not based solely on automated decision-making.

Appendix 7: Data processing by external suppliers' procedure

1. **Purpose**

The purpose of this procedure is to outline the steps and guidelines for the processing of personal data by external suppliers on behalf of WFSA. This procedure aims to ensure that personal data is processed in a lawful, secure, and compliant manner, in accordance with applicable data protection laws, including the UK General Data Protection Regulation (UK-GDPR).

2. Scope

This procedure covers all situations where external suppliers are used by WFSA to process personal data on its behalf.

3. Responsibilities

The Finance & Operations Manager is responsible for approving all subcontractors used by WFSA for processing personal data, in accordance with this procedure.

The owners of third-party relationships must ensure that all data processing by third parties complies with this procedure.

Laurie Barnes will assist the third-party relationship owner by providing technical and other resources as needed.

Regular audits of third-party compliance will be conducted by the Finance & Operations Manager.

4. Procedure

WFSA will only engage with third-party data processors that can provide adequate security measures (technical, physical, or organisational) for all personal data they process on behalf of WFSA.

In addition to other circumstances set out elsewhere in this procedure, WFSA shall only engage with third party processors outside of the UK in the following circumstances:

- When the third-party data processor has been identified positively in an adequacy decision; or

- When the rights and freedoms of data subject are secured by legally binding corporate rules and other safeguards, agreed between WFSA and the third-party data processor and are equal or equivalent to those afforded by the UK; or

- Where a specific arrangement between WFSA and the third-party data processor has been approved by the Information Commissioner or the supervisory authority.

Before entering into any agreement with a third-party data processor, WFSA must carry out an information security risk assessment.

Taking into consideration the basis of the nature of the personal data to be processed and the specific circumstances of the data processing, WFSA may deem it necessary that an additional audit of the third-party data processor's security arrangements may be carried out before entering into any agreement.

WFSA shall only engage a third-party processor pursuant to a written contract which expressly sets out the service to be provided. The third-party processor is also required to provide suitable security for the personal data to be processed, which must also be confirmed in the written contract ("the data processing contract").

WFSA is required to carry out regular audits of the third-party data processor's security arrangements throughout the duration of the contract, when the third party has access to personal data held by WFSA.

The data processing contract must contain a clause preventing third-party data processors from hiring subcontractors for the processing of personal data in the absence of express, written approval by WFSA.

WFSA will only approve contracts with second-tier data processors, if the subcontractors of the third-party data processor agree to provide the same level of security and protection to the rights and freedoms of the data subject as those afforded by WFSA. In addition, the contract between the third-party data processor and the second-tier data processors must contain a clause requiring that all personal data will be either destroyed or returned to WFSA upon the termination of the contract.

5. Termination

In the event of any termination of a data processing agreement the third party shall:

- Immediately cease processing the personal data
- Promptly destroy or return all copies of the personal data and certify to WFSA that it has done so, unless it is prevented by law or any regulatory authority from destroying or returning all or part of such data, in which case it shall keep such data confidential and shall not process it further.

6. Document owner

The CEO is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated June 2024 is available to all employees of WFSA as part of the staff handbook.

This policy document was approved by WFSA's Board and is issued by Laurie Barnes on a version-controlled basis.

Appendix 8: Fair processing procedure

1. Purpose

The purpose of this Fair Processing Procedure is to provide guidelines for the fair and transparent processing of personal data by WFSA. This procedure aims to ensure compliance with applicable data protection laws, including the UK General Data Protection Regulation (UK-GDPR), and to uphold individuals' rights and privacy.

2. Scope

The scope of this procedure encompasses all information processing of data subjects by WFSA.

3. Fair Processing Notice

Responsibility for the Fair Processing Notice rests with WFSA's CEO who must ensure that it is factually correct and that appropriate mechanisms are in place to ensure that all data subjects are aware of its contents prior to the commencement of WFSA's data collection.

4. Procedure

Personal data may only be processed upon receipt of authorisation from the CEO.

The following information must be provided to data subjects prior to data collection, in plain and clear language:

1. Organisation Name, including contact details;

2. Objective behind the processing of personal information;

3. Duration of time the personal data will be stored for and the storage criteria;

4. Statement regarding the disclosure of personal information to third parties;

5. Information regarding the rights of data subjects in respect of their personal data, including but not limited to:
    - The right to access personal information;
    - The right to withdraw consent;
    - The right to amend personal data;
    - The right to request that personal data be permanently deleted;

- The right to strict processing; and
- The right to raise an official complaint with the relevant authority;

6. Information in relation to any automated processing, for instance profiling, to be carried out, if relevant;

7. Whether personal data must be provided for the purposes of fulfilling or entering into a contract and the outcome should the data subject refuse to provide personal data;

8. Details regarding the destination of the personal data:
    - Whether personal data will be transferred outside of the UK; and
    - Whether an adequacy decision has been made regarding the destination of the data; and/or
    - Whether any safeguards are in place to ensure the adequacy of the destination; and

9. Any other material that would ensure that the data processing is fair at all times.

All data subjects must be notified prior to the processing of their personal data by the WFSA Foundation via a FAIR PROCESSING NOTICE, containing the following statements:

For marketing use, whether currently or in the future:

"Please note that your personal information may be used for marketing purposes. We may contact you via email to provide information and updates about WFSA's work and activities worldwide. This is not obligatory, and you may opt out by emailing Laurie Barnes, requesting that your personal information be removed. You may also unsubscribe from our electronic marketing content at any time, by selecting the unsubscribe option."

For marketing use, when specific consent has been provided by the data subject:

"Please note that you have provided explicit consent for the use of your personal information by WFSA for marketing use. We will contact you by email to provide information and updates about WFSA's work and activities worldwide, including how to donate to support these. You may withdraw your consent by emailing: Laurie Barnes *at any time and you will be immediately withdrawn from all of our marketing lists."*

5. Responsibilities of person responsible for data protection

1. *Consent procedures:* To incorporate procedures in relation to personal data processing based on consent, ensuring that processing ceases when consent is withdrawn;

2. *Consent withdrawal:* To monitor all requests withdrawing consent by keeping a register of all relevant requests and ensuring that all requests are actioned within 24 hours;

3. *Explicit consent:* To ensure that the Fair Processing Notice contains relevant procedures for receiving the relevant consent, when explicit consent is required for marketing purposes due to sectoral requirements or legislation;

4. *Sensitive personal data:* To ensure that the Fair Processing Notice sets out explicitly the purpose or purposes for which sensitive personal data will, or may, be used, when sensitive personal information is collected for a specific purpose or purposes;

5. *Parental consent:* To ensure that parental consent has been provided in relation to all data subjects 16 years of age, or younger;

6. *Data protection law:* To ensure that all new data collection methods comply with data protection laws and good practice, by reviewing and signing off all new such methods;

7. *Fair Processing Notice register:* To maintain a Fair Processing Notice register of all Fair Processing Notices issued, setting out the following information:
    - Fair Processing Notice version number;
    - Issue date and withdrawal date;
    - Location where data will be used;
    - Purpose for which personal data is collected; and
    - Description of expressions, foreign language or formatting, to ensure that the Fair Processing Notice can be fully understood by the target group.

8. *Specified purpose:* To approve all written requests for changes to the purpose of process of personal data and determine if additional consent is required from the data subject:
    - In the event that additional consent is required, to determine the form of the consent and the protocol to be followed by WFSA to ensure that the data subject is informed of the new purpose and has provided the necessary consent;
    - To identify a relevant exemption, when applicable, in the Authorisation to Process; and

- To update the Data Inventory Schedule by setting out details of the new purpose, referring directly to the Authorisation to Process; and

9. *Data protection:* To ensure that personal data that is shared with a third party complies with WFSA's notification to the ICO and with the terms of the Fair Processing Notice previously provided to the data subject and any relevant consents provided by the data subject:

    - To ensure that an agreement drafted by WFSA's legal advisors is entered into with the third party, setting out the purpose or purposes for which the information will, or may be, used and listing any restrictions or limitations on the use of the personal information for other purposes;
    - To ensure that the agreement contains an undertaking, or other applicable evidence, by the third party that it is committed to processing its data in such a way that it adheres to the requirements of the DPA at all times;
    - To ensure the agreement contains appropriate controls and safeguards to ensure the protection of personal information pursuant to the UK-GDPR, when such information may be legally shared without the consent of the data subject; and
    - To ensure that any data profiles created by matching data collected by WFSA with other data are not used outside of the context of the ICO notification and the consents of the data subject.

Appendix 9: Privacy Impact Assessment

1. Purpose

The purpose of this Privacy Impact Assessment (PIA) is to identify and assess the potential privacy risks and impacts associated with a specific project, initiative, or system implementation undertaken by WFSA. This assessment aims to ensure compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR), and to mitigate any adverse effects on individuals' privacy.

2. Scope

WFSA's data processing activities will undergo an initial Privacy Impact Assessment ("PIA") and subsequent PIAs throughout its lifecycle.

A subsequent PIA may be carried out in the following circumstances:

- When setting up a new IT system;
- When new legislation, policies or related matters affecting privacy, are developed;
- When launching a data sharing initiative; and/or
- When personal data is used for new purposes.

3. Responsibilities

The person with responsibility for data protection in WFSA, currently Laurie Barnes, is responsible for determining whether a full PIA is required. They shall reach this decision based on a PIA questionnaire, which must be undertaken for the purposes of making such a determination.

All completed PIAs will be signed off by the Board.

4. Process

The CEO shall at all times direct Laurie Barnes to conduct PIAs by direct reference to the Information Commissioner's Office ("ICO") Code of Practice.

Laurie Barnes may seek specialist advice regarding privacy, should they feel it is required. Laurie Barnes should record all outcomes, including whether or not a PIA is required, in the ICO Code of Practice Annexes. Laurie Barnes shall record in all change control processes that a PIA has been considered.

Appendix 10: Third Party Access to Data

1. Purpose: The purpose of this Third Party Access to Data Procedure is to establish guidelines for granting and managing access to WFSA's data by third-party entities. This procedure aims to ensure the secure and compliant handling of data shared with external parties, protecting the privacy and confidentiality of the data, and complying with applicable data protection laws, including the General Data Protection Regulation (GDPR).

2. Scope

WFSA is responsible for ensuring the security of its data processing facilities and other information assets in relation to third parties. This procedure applies to all situations where third parties require access to any of WFSA's data, including all of the following categories of external parties with whom WFSA may have agreements in place:

- Service providers, including managed security service providers;
- Clients and customers;
- Outsourcing suppliers including: facilities, operations, IT systems, data collection and call centers;
- Consultants;
- Auditors;
- Providers of IT systems and services;
- Providers of cleaning, catering and other outsourced support services; and
- Temporary staff, including placement and other short-term appointments.

WFSA is responsible for assessing associated third-party risks according to the category and level of risk involved.

3. Responsibilities

Where there is a business requirement to work with third parties, WFSA is required to enter into a formal agreement regarding information security with all third-party service providers.

The person with responsibility for data protection, currently Laurie Barnes, and all third-party relationship owners responsible for the aforementioned service categories are required to ensure that formal external party contracts are entered into in line with this procedure. All contracts must implement adequate security controls, delivery levels and service definitions and Laurie Barnes and third-party relationship owners are responsible for ensuring that these are properly

implemented and maintained by the third party, carrying out risk assessments as and when required by this procedure.

Throughout any transition periods, WFSA shall offer the same level of security.

4. Procedure

WFSA shall only grant third parties access to organisational assets, including personal data and other information, once a risk assessment has been carried out and the appropriate systems and controls are implemented.

Risk assessment - step by step

1. WFSA carries out a risk assessment and identifies all risks pursuant to third party access to data.

2. For each third party, the risk assessment shall identify the following:

    - The data and the processing facilities which the third party will have access to;
    - The type of access the third party shall have, whether physical and/or logical, whether on or off-site;
    - The exact location from which the third party will access the data;
    - The value and specific classification of the information which the third party will access;
    - The data to which the third party shall not be granted access and which may need to be secured by additional means;
    - A full list of the third party's personnel who will be or are likely to be involved in the access to data, including partners and external contractors;
    - How the third party's personnel shall be authenticated;
    - How the third party intends to store, process and communicate the data;
    - The impact that inaccurate, incorrect or misleading data shared with the third party would have on the third party;
    - The impact on the third party of a potential inability to access the data when required;
    - How WFSA's Security Incident Management Procedure applies and should be implemented if and when information security incidents take place, which involve the third party;
    - Any legal or regulatory matters regarding the third party that are of note; and

- How WFSA's stakeholder interests may be affected by any of the decisions made in relation to the third party relationship.

3. All systems and controls implemented by WFSA pursuant to the risk assessment must be according to the UK GDPR and must be within the power of WFSA.

4. WFSA and the third party agree to implement appropriate controls and WFSA's legal advisors shall draw up a contract, which the third party is required to sign. Amongst the third party's obligations is the requirement that all of its personnel are aware of their obligations pursuant to the contract.

5. When drafting the contract, WFSA's legal advisers are required to consider and include all of the following information security policy matters and insofar as any matters are not included within the contract, must provide a documented reason why they were not included, as well as the requirement under which they were identified as part of the risk assessment:

    - A clear definition and/or description of the service or product provided by the third party and a description of the data and its classification;
    - Training, education and awareness requirements for all third party users;
    - Any provisions for the transfer of personnel;
    - Responsibilities for the installation of software and hardware, as well as maintenance and destruction;
    - A robust and clearly defined process of reporting, including structural requirements, reporting formats and escalation protocols;
    - A requirement that the third party adequately resources reporting, monitoring and compliance activities;
    - A robust and clearly defined change management process;
    - An Access Control Policy, refer to Security Access Policy;
    - Physical controls, including secure areas;
    - Controls against malware;
    - Data security incident management;
    - Appropriate service and security levels, including what would amount to unacceptable service and security, as well as a clearly defined verifiable criteria of performance and security, monitoring and reporting;
    - The right for WFSA to monitor and audit the performance of the third party, for which WFSA may use external auditors, including the third party's processes for change

management, identifying vulnerabilities and managing information security incidents, as well as WFSA's right to revoke activities;
- The requirements of service continuity;
- Legal responsibilities and liabilities and how they shall be met;
- Copyright and Intellectual Property Rights protection;
- Systems and controls in relation to subcontractors; and
- Conditions for renegotiation and termination of agreements and contingency plans.

5. Information transfer agreements

When the contract between the WFSA and a third party is for the transfer of data or software, the following additional controls must be considered, pursuant to an individual risk assessment:

- How the management of both WFSA and of the third party shall be responsible for notifying transmission, dispatch and receipt of data as well as any associated procedures and controls;
- Systems and procedures for ensuring the traceability and non-repudiation of data;
- The means of data transmission;
- Packaging of data;
- Agreed system of labelling the data;
- The selection of couriers and methods of identification;
- The management of data security incidents;
- Escrow agreements;
- Copyright, data protection and software licensing;
- Technical requirements for recording or reading data or software; and
- Any other systems and controls such the use of cryptography.

6. Managing changes to third party services

Please also refer to the WFSA Security Access Policy.

WFSA may need to agree to variations to contracts with third parties, as a result of the following potential changes:

- The service it currently offers;
- The implementation of new systems or applications;
- Updates or modifications to its policies and procedures; and

- Updated systems and controls arising from new risk assessments or data security incidents.

A third party may require changes to its contract with the WFSA as a result of the following potential changes:

- New networks and infrastructure;
- New technologies, products or new releases of current products;
- New physical locations;
- New physical services;
- New tools or methodologies;
- New service providers; and
- New suppliers of hardware or software.

If any changes arise, a new risk assessment and review of the selected controls must be carried out. Any changes to the contract based on the introduction of new controls, or the amendment of existing controls must be agreed with the third party and inserted into the contract via an agreed variation.

Laurie Barnes and relationship owners are responsible for ensuring that the new controls are implemented and incorporated into review and monitoring arrangements already in place.

7. Document owner

The CEO is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated June 2024 is available to all employees of WFSA as part of the staff handbook.

This policy document was approved by WFSA's Board and is issued by the CEO on a version-controlled basis.

Appendix 11: Employee Privacy Notice

WFSA is aware of its obligations under the UK General Data Protection Regulation (UK-GDPR) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with the UK-GDPR, the types of data that we hold about you as an employee of WFSA. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This notice applies to current and former employees, workers and contractors.

Data controller details

WFSA is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows:

WFSA
39-41, The Busworks,
North Road,
London N7 9DP,
United Kingdom

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed

Types of data we process

We hold many types of data about you, including:

- your personal details including your name, address, date of birth, email address, phone numbers
- gender

- your photograph
- marital status
- dependents, next of kin and their contact numbers
- medical or health information including whether or not you have a disability
- information used for equal opportunities monitoring about your sexual orientation, religion or belief and ethnic origin
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK
- bank details
- tax codes
- National Insurance number
- current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to your employment with us
- letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings
- internal performance information including measurements against targets, formal warnings and related documentation with regard to capability procedures, appraisal forms
- leave records including annual leave, family leave, sickness absence etc.
- training details
- building entry card records.

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting managers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next-of-kin details. Other details may be collected directly from you in the form of official documentation such as your driving license, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files or within WFSA HR and IT systems.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- to protect your interests and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- carry out the employment contract that we have entered into with you and
- ensure you are paid.

We also need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid
- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of WFSA. We have set these out below:

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc.
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- assessing training needs
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments

- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave and pay etc
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access

Special categories of data

Special categories of data are data relating to e.g. your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

- in our sickness absence management procedures
- to determine reasonable adjustments

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you

will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment. We use criminal conviction data in the following ways:

- both to ensure your right to work in the UK and any interaction with vulnerable groups

We process this data because of our legal obligation to comply with legislation regarding the right to work in the UK and our duty to provide a safe environment for work.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties, e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information e.g. confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

Sharing your data

Your data will be shared with colleagues within WFSA where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management of you, the Governance Officer for maintaining personnel records. and our payroll and pension providers for administering payment under your contract of employment.

We share your data with third parties in order to for example obtain references as part of the recruitment process, with our payroll provider to ensure you are paid, with our pension provider to ensure correct pension deductions are made in accordance with existing legislation.

We may also share your data with third parties as part of an organisational restructure, or for other reasons to comply with a legal obligation upon us.

We may on occasion share your data with bodies outside of the UK. Please be assured that measures have been put in place, as outlined by the policy, to ensure that your data is transferred

securely and that the bodies who receive the data that we have transferred process it in a way required by UK data protection laws:

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such occurrences.

Where we share your data with third parties, we provide written instructions to them to ensure that your data is held securely and in line with the UK-GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in some cases we will keep your data for a period after your employment has ended. Retention periods can vary depending on why we need your data. Please refer to our data retention policy for more detailed information. This policy can be found within the staff handbook.

Automated decision-making

No decision will be made about you solely on the basis of automated decision-making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold about you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our Data Subject Access Request policy which can be provided by Laurie Barnes.
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it

- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold about you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision-making in a way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us your consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact Laurie Barnes.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

Data protection compliance

Laurie Barnes is the WFSA appointed compliance officer in respect of its data protection activities.

Change history record

Issue	Description of Change	Approval	Date of Issue
1	Issue	Board	August 2024
2			
3			