Wells United Charities

Charity Number: 236897

DATA PROTECTION (including GDPR) POLICY

This policy was created and ratified by Trustees on and will be reviewed annually	July 2021
Responsible person for updating:	**Data Protection Officer**
This policy will be reviewed by Trustees annually and when amendments are made to national advice and guidance.	

Associated Documentation

Guide to GDPR provided by Gov.uk

Contents

1. Aims

WUC aims to ensure that all personal data collected, stored and processed is done so in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the Trust's use of biometric data.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

WUC processes personal data relating to adults, children, members and Trustees and is therefore deemed to be the data controller.

5. Roles and Responsibilities

This policy applies to **all Trustees** and to external organisations or individuals working on the Charitie's behalf. Trustees who do not comply with this policy may face disciplinary action or be required to relinquish their position of Trustee.

5.1. Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the relevant governing board and, where relevant, report to the Trustees their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Alastair Ogle.

5.2. Trustees

Trustees are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the Chair of Trustees of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles that WUC must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure
- Must not be transferred to people of organisations situated in other countries without adequate protection

This policy sets out how WUC aims to comply with these principles.

7. Collecting Personal Data

7.1. Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that WUC can **fulfil a contract** with the individual, or the individual has asked WUC to take specific steps before entering into a contract
- The data needs to be processed so that WUC can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the charity can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of WUC or a third party (Provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2. Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Trustees must only process personal data where it is necessary in order to do their jobs.

When Trustees no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a member or trustee or beneficiary that puts their safety at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our members of beneficiaries– for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided
- The interests of public health, including NHS Test and Trace

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our volunteers, members volunteers, grant recipients or supporters.

Where we transfer personal data to a country or territory outside the UK we will do so in accordance with data protection law.

9. Subject Access Requests and other Rights of Individuals

9.1. Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that WUC holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If trustees receive a subject access request, they must immediately forward it to the DPO.

9.2. Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents / carers may not be granted if their child is aged 12 or above. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3. Responding to Subject Access Requests When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that an individual is at risk of abuse, where the disclosure of that information would not be in the individuals best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning a child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4. Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Right to fair and transparent processing
- Right of access
- Right of rectification
- Right to erasure (the 'right to be forgotten')
- Right to restrict processing
- Right to be notified of erasure, rectification or restriction
- Right of data portability

- Right to object to processing
- Right to object to processing for scientific, historical or statistical purposes
- Right to not be evaluated on the basis of automated processing
- Right to withdraw consent at any time
- Right to be notified about a data breach
- Right to be an effective judicial remedy again a supervisory authority
- Right to lodge a complaint with supervisory authority
- Right to an effective judicial remedy against a controller or processor
- Right to compensation

Individuals should submit any request to exercise these rights to the DPO.

10. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks or left anywhere else where there is general access
- Personal information must not be left unattended or insecure at anytime.
- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Trustees are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Trustees who store personal information on their personal devices are expected to follow the same security procedures
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

11. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on behalf of WUC and its establishments. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

12. Personal Data Breaches

The Trustees will make all reasonable endeavours to ensure that there are no personal data breaches.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an establishment context may include, but are not limited to:

- A non-anonymised dataset being published on the charity website
- Safeguarding information being made available to an unauthorised person
- The theft of a laptop belonging to Trustees

13. Training

All Trustees will complete data protection training as part of their induction process and this will be updated annually. Data protection will also form part of training updates where changes to legislation, guidance or the Trust or its establishment's processes make it necessary.

14. Monitoring and Review of Policy

The Trustees will review this policy every year and assess its effectiveness and implementation. Any deficiencies identified shall be corrected and used to inform review of the policy, which will be promoted and implemented throughout the Trust.