DATA PROTECTION POLICY

Policy Statement

Wycombe Youth Action ('WYA') is fully committed to and compliant with the requirements of the 2018 General Data Protection Regulation (GDPR). The charity will follow procedures that aim to ensure that all individuals who have access to any personal data held by or on behalf of the charity are fully aware of and abide by their duties and responsibilities under the above Regulation.

WYA regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between the charity, its employees, clients and temporary workers. The charity will therefore ensure that it treats personal information lawfully and correctly. To this end the company fully endorses and adheres to the principles of the GDPR.

WYA holds sensitive and/or confidential data relating to details about the young people it works with and has clearly documented procedures in place for creation, storage, use, sharing/handover and destruction of such data as well as safeguarding procedures, which compliment the GDPR guidelines.

Scope of the Policy

In order to operate efficiently, WYA has to collect and use information about the people with whom it works.

Sensitive data and personal information is handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

All employees are required to comply with this policy when dealing with other employees, temporary staff, consultants, job applicants, clients, third parties, and contacts of the charity, and anyone else with whom they come into contact during the course of their employment.

All employees are made fully aware of this policy and of their duties and responsibilities under the GDPR.

Data

In considering our Data Policy we reviewed the data that we need in order to run our projects well and safely. A review of the type of data that's necessary is taken as part of the annual review of the Data Protection Policy.

Below is a table setting out the list of data that is collected for the purpose of running the groups and projects of WYA:

Data type	**Lawful reason for collecting it**	**Purpose**
Names and contact details (including emergency contact)	Consent	Safeguarding and to fulfil WYA's purpose
Ethnicity	Consent	For equal opportunities
Sexual orientation	Consent	To consider when planning which project a client should attend
Religion	Consent	To consider when planning which project a client should attend
Date of birth	Consent	To ensure the individual is invited to age-appropriate events
Project attendance	Consent	To monitor attendance of projects
Emails/correspondence	Consent	To maintain contact
Notes/documentation re clients	Consent	To manage the progress of an individual

Data concerning young people is held for a minimum of fifty years after the individual stops attending any projects as part of our safeguarding procedures.

Responsibilities

It is the direct responsibility of the Data Protection Officer to work with the Office Manager to ensure the implementation of this policy on a day-to-day basis; however, all employees have a responsibility to accept their personal involvement in applying it and must be familiar with the policy and ensure that it is followed by both themselves and employees for whom they have a responsibility.

The Data Protection Officer for WYA is Sarah Lawton.

Disciplinary action may be taken against any employee who acts in breach of this policy. Disciplinary action may include summary dismissal in the case of a serious breach of this policy or repeated breaches. In other cases, it may include a verbal or written warning. Such action will be taken in accordance with the Company's disciplinary procedure.

The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with eight legally enforceable principles of good practice which require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
4. Shall be accurate and where necessary, kept up to date.
5. Shall not be kept for longer than is necessary for that purpose or those purposes.
6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure i.e. protected by an appropriate degree of security.
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Handling of Personal Data

WYA, through appropriate management and the use of strict criteria and controls:

1. Observes fully the conditions regarding the fair collection and use of personal information.
2. Meets its legal obligations to specify the purpose for which information is used.
3. Collects and processes appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
4. Only collects data at the individuals consent as part of the criteria for joining a project.
5. Ensures the quality of information used.
6. Applies strict checks to determine the length of time information is held.
7. Takes appropriate technical and organisational security measures to safeguard personal information.
8. Ensures that personal information is not transferred abroad without suitable safeguards.
9. Ensures that the rights of people about whom the information is held can be fully exercised under the Regulation. These include:
    - The right to be informed that processing is being undertaken.
    - The right of access to one's personal information within the statutory month.
    - The right to prevent processing.
    - The right to correct, rectify, block or erase information regarded as wrong information.
10. Reviews the data that has been collected periodically to ensure it is still relevant and required.

In addition, WYA ensures that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.

- Everyone managing and handling personal information is appropriately supervised.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data is in compliance with approved procedures.

All employees take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular they ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically.
- Personal data is held on the network or cloud where appropriate security measures have been put in place to ensure access is restricted to authorised individuals.
- Individual passwords are updated regularly as prompted and are not straightforward or easy to work out.
- Individual passwords are not shared and are such that they are not easily compromised.
- Consideration is taken at all times, of who is able to see their computer screen and that the screens are locked whenever they are away from their desk.
- Staff sign non-disclosure agreements to protect both the charity and client sensitive / confidential data.

Any contractors who are users of personal information supplied by WYA are required to sign a non-disclosure agreement confirming that they will abide by the requirements of the GDPR with regard to information supplied by the company. Where it is necessary for contractors to be supplied with any sensitive/confidential data, they are asked to supply their GDPR policy to confirm they are complying with all aspects set out in the GDPR. Contractors are given their own passwords and access to the systems, and this access will be controlled by the Office Manager. The charity takes responsibility to ensure this access is revoked when the contract is finished.

Personal data is collected via direct referral from the young person, parent or a third party such as the police and access and processing of data is only carried out by staff for the purposes outlined in the Data Review Spreadsheet which is kept on BreatheHR.

WYA may be required to disclose personal data by law in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law, by order of a court of competent jurisdiction, or in connection with legal proceedings.
In this situation, legal advice may be sought.

For the duration that WYA is obliged to hold personal data, the charity will use reasonable endeavours to ensure that personal data is maintained and up to date; however, individuals are made aware they are under a duty to inform the charity of any and all

changes to their personal data to ensure that it is up to date, and they will update or delete their personal data accordingly. If WYA has no contact with the individual to whom the personal data relates, then following the expiry of a reasonable period as they consider appropriate, they archive or may delete it. After an appropriate period, they contact the individual to whom the personal data relates and ask if they wish for their personal data to be maintained on the database.

All client, contact, consultant, contractor and third party personal and sensitive / confidential data is held on the CRM system and is processed via email, CRM system and telephone.

The charity reserves the right to transfer information (including personal data) to a third party in the event of a sale, merger, liquidation, receivership, or transfer of all or substantially all of the assets of our company, provided that the third party agrees to adhere to the terms of this Data Protection Policy and provided that the third party only uses such personal data for the purposes that it was provided it to them. In such event, legal advice will be sought and the individual to whom the personal data relates will be notified of any such transfer and they will be afforded an opportunity to opt-out.

Sensitive Personal Data

Data in respect of the following is defined as "sensitive personal data":

- the racial or ethnic origin of the data subject,
- his/her political opinions,
- his/her religious beliefs or other beliefs of a similar nature,
- whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his/her physical or mental health or condition,
- his/her sexual life,
- the commission or alleged commission by him/her of any offence, or
- proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

The presumption is that, because information about these matters could be used in a discriminatory way and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

In line with the GDPR conditions for processing sensitive personal data, WYA always obtains explicit consent to the processing from the individual about whom the sensitive personal data relates and, where possible, will only hold this information if there is more than one lawful reason to do so.

Safeguarding and 13-16yr olds

The GDPR in the UK states that anyone over the age of 13yrs may give consent for their data to be stored and processed. However, it also is clear that, where there are safeguarding concerns the regulations around safeguarding override those of GDPR.

The young people that WYA work with would often be referred to as vulnerable and therefore anyone under the age of 16yrs old must have the consent of an adult to have their data stored and processed by WYA.

Access by Data Subjects

A data subject may make a subject access request ("SAR") at any time to see the information which the Company holds about them. SARs must be made in writing.

Upon receipt of a SAR the Data Protection Controller/Officer shall consider the request and respond within the maximum period of one month, giving a full explanation if such a request is refused.

It is noted that, where multiple requests are received by the same individual in a short period of time for access, this could be considered a reason to refuse the request.

Records Management

WYA records management procedure is designed to ensure that each record is managed through its life cycle from creation or receipt through maintenance and use to disposal or deletion. The charity focuses on:

- Creating appropriate records and maintaining these on the systems.
- Updating the information provided, accurately.
- Reviewing the information held on a regular basis.
- Ensuring records are located correctly to enable ease of access and retrieval.
- Controlling the timescale and method for destruction of information.
- Managing information security to ensure personal, sensitive, and confidential data is safe and secure from malicious access.

Each member of staff has their own individual login to the system.

Records can be received in hard copy or electronically and are scanned and uploaded or saved against the relevant individual. The majority of documentation is held electronically. Paper documentation includes any original documentation that must be retained on paper (e.g. documents with wet signatures).

As part of induction training, all staff are asked to read and sign the GDPR Policy and Procedures to confirm they understand and agree to comply with them.

An audit may be taken of the data held by WYA and this will be carried out by the Data Protection Officer. This audit will be at least once every two years but may be more often as

considered necessary.

Disposal of Records

Electronic records are deleted as appropriate and minimum records are maintained of the deletion, as set out in the GDPR.

Paper records are shredded using a criss-cross shredder or via an external agency, and a certificate is sought as proof of disposal.

Reporting a Data Breach

A 'data breach' is defined by the ICO as 'a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.'

It is the responsibility of every member of staff of WYA to report any data breach or suspected data breach to the Data Protection Officer as soon as possible, giving full details of what happened to cause the breach, what data may have been breached and any other details that are relevant to the situation.

The Data Protection Officer and the Office Manager will work together to establish the facts and agree the impact on rights and freedoms of those affected and whether they need to be informed of the breach. Where a Data Breach is deemed to have occurred the Data Protection Officer has 72 hrs to report it to the ICO from the time that they were made aware of it making them aware of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records involved.
- The name and contact details of the Data Protection Officer where more information can be obtained.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

It may be necessary to advise those whose data has been breached of the event. When advising them the following information will be provided:

- the name and contact details of the Data Protection Officer where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

If possible, advice will be given to individuals on the steps they can take to protect themselves, and what WYA will do to help them. Depending on the circumstances, this may include such things as:

- forcing a password reset;
- advising individuals to use strong, unique passwords; and
- telling them to look out for phishing emails or fraudulent activity on their accounts.

Whether a breach is considered 'reportable' or not, a record will be kept of the full details, with date and times. The Data Protection Officer should be informed of all incidents and will discuss any extra security measures to be taken, with the Office Manager.

Use of Cookies & Similar Technologies

Cookies are small text files that are placed on a computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. The list below explains examples of cookies we may use and why.

Most web browsers allow you to modify your preferences to notify you when a cookie is set, or to reject all cookies. Restricting or rejecting cookies on WYA website will mean that certain areas of the site will not function correctly. Further information can be found on our website.

Analytics
This is a small cookie that allows the site owner to check which pages are the most popular on the site and so provide more site content that is popular to users. It contains no personal or private data at all and is used on millions of websites worldwide.

Specific Technologies

WYA uses a customised CRM system to store all data in and to share information with any relevant parties. This CRM is GDPR compliant and has security measures in place to ensure all information is kept secure for as long as it is in WYA's possession.

Only staff requiring access to the database, have access each with their own individual passwords. Passwords should not be shared.

WYA also uses Upshot, which is a secure system managed by LEAP, which is the brand name for Bucks & MK Sport and Activity Partnership to process data of individuals involved in their Children and Young People projects.

Implementation

The Data Controller is responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Data Protection Officer who has overall responsibility for:

- The provision of records management and data protection training, for staff within the company.
- The development of best practice guidelines.
- Carrying out compliance checks to ensure adherence with the GDPR.
- Ensuring all staff sign the company's confidentiality agreement and understand the penalties for deliberate misuse, damage, theft or destruction of records.

Review

This policy will be reviewed annually, in September, and may be altered from time to time in light of legislative changes or other prevailing circumstances. All staff will be informed of any changes to the policy.

Date of next review: October 2023

Review date:	**26 October 2022**
By:	**Sarah Lawton**
Designation:	**Data Protection Officer**

Review date:	**30 November 2021**
By:	**Sarah Lawton**
Designation:	**Data Protection Officer**

Name:	**Sarah Lawton**
Designation:	**Data Protection Officer**
Date:	**10 September 2020**