DATA PROTECTION PROCEDURES

Procedure Statement

Wycombe Youth Action (WYA) is fully committed to and compliant with the requirements of the General Data Protection Regulation (GDPR) 2018. WYA therefore follows procedures that aim to ensure that the charity complies with the scope of the GDPR. As WYA holds items of information that would be classed as 'special category data' extra consideration is given to protecting individuals from these being revealed to others.

WYA regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between its clients and contacts. To this end WYA fully endorses and adheres to the Principles of Data Protection as set out in the General Data Protection Regulation 2018.

The procedures below set out how WYA complies with the scope of the GDPR.

Data collection

Young people

- A young person can refer themselves to WYA.
- Referrals also come from a parent, guardian or a third party such as the school, police or social services.
- They are asked to complete forms asking for permission to hold and use their data and to take and use their photos for social media. Anyone under 18yrs is asked for parental consent before any data is processed.
- Data is uploaded to the WYA CRM system once consent has been received and the paper forms are disposed of as set out in the Data Review spreadsheet.

Contacts and partners

- Where WYA partner with other agencies or funders, their details are held on the CRM system as set out in the Data Review spreadsheet.

HR

- When CVs are submitted, they are saved and stored securely as soon as possible.
- Only those involved in the recruitment process are allowed access and do not share confidential information to anyone outside of the process, unless considered to need to know it.
- All HR data is stored on the HR database, BreatheHR.
- Details of where it will be stored and how long it will be kept are found on the Data Review spreadsheet.

Security of data

- Wherever possible data should be stored securely, ideally on the CRM system.
- All devices holding data should be protected with anti-virus, malware and any other protection required.
- Data stored on an individuals' computer or phone should only be in exceptional circumstances for the minimum amount of time, and only on devices that are encrypted and password protected.
- If any mobile devices are taken away from the office, containing personal data, extra consideration should be taken to ensure the security of the device during the time it is out of the office.
- Staff should be mindful of who can see their computer screens at all times and ensure they 'lock' their computers when they are away from their desk, to prevent an unauthorised person from gaining access.
- Passwords should be changed regularly and should not be easy to break.
- Passwords should never be shared with anyone.
- Confidential paper files should be kept locked away and access minimised to those who require it.
- See 'communication/sharing of data' for details around transferring personal data from one system to another.

Destruction of data

- Electronic files should be deleted in accordance with the data spreadsheet, and 'trash' files cleared regularly.
- Paper files should be shredded in a criss-cross shredder or using a shredding service. Note, where a shredding service is used, a certificate should be obtained, and filed, giving proof that they paperwork has been destroyed appropriately.

Communication/sharing of data

Communication

- Where possible, email should not be not used for transferring personal information.
- Email may be used to communicate to young people and, if an email is going to more than one person all recipients will be blind copied.
- Personal data should not be shared with anyone outside of WYA without the permission of the individual, unless there is a legal reason for doing so and this should only be done under advisement from either the Data Protection Officer, Office Manager, Chairwoman or Trustees of the Charity.
- Where an individuals' information is to be uploaded to 'Upshot, the database run by 'Leap', a project run by Bucks Council, the individual should be advised of this and asked for permission to do so.

Data Sharing

- Any data that is to be shared should always be done so in an encrypted file or uploaded to a web-based system, where it can benefit from maximum protection.
- Where data is sent on to a third party confirmation should be obtained to ensure they are committed to handling the data within the guidelines of GDPR.

Individual rights

Under GDPR every individual has a number of 'rights'. WYA recognises that the individual rights are the entitlement of every individual including clients, staff, contractors or third parties. To ensure the firm meets those rights, the following procedures are in place:

1. The Right to be Informed
    - All young people will be asked to sign a consent form confirming that their information may be stored and processed, giving information about where the data will be held and for what purpose.
    - Unless safeguarding rules apply or there is a legal reason, all individuals will be advised if their data is being shared with a third party.
2. The Right to access
    - When someone asks for access to the personal data WYA holds on them, WYA will ask them to send their request in writing.
    - WYA may ask for ID to prove they are the individual.
    - WYA will review the data to ensure it does not conflict with another persons' rights, ie if there is another person mentioned in the data.
    - Generally, access would be given electronically either by giving the individual access to their personal details or by sending them a downloaded copy.
    - WYA will ensure the individual is given access to their data within one month of the request.
    - Where WYA are not in agreement with giving access or the access would compromise another individual's rights, WYA will arrange to talk to the client as soon as possible to discuss the situation, and, if necessary, WYA will take external advice as a matter of priority and, in this situation we may need to extend the period before the access is given.
3. The Right to rectification
    - When someone asks WYA to rectify the personal data WYA holds on them, they will ask the individual to send their request in writing.
    - WYA may ask for ID to confirm they are the individual.
    - WYA will make the rectification in all areas that the data is stored within one month of the request and confirm that the rectification has been carried out.
    - Where the charity is not in agreement with the rectification, they will arrange to talk to the client as soon as possible to discuss the situation, and, if necessary, WYA will take external advice as a matter of priority and, in this situation the charity may need to extend the period before the rectification is carried out.
    - Every 5 years, WYA will check with their contacts that the data they still hold on them is correct.

4. The Right to data portability
    - When someone asks to have their personal data available for them to send to another system, WYA will ask them to send their request in writing.
    - WYA may ask for ID to confirm they are the individual.
    - WYA will review the data to ensure it does not conflict with another persons' rights, ie if there is another person mentioned in the data.
    - This would then be supplied via a recognised 'machine readable' format, ie CSV, XML etc either to the individual or directly to the other Controller.
    - WYA will ensure the request is actioned within one month of the request.
    - Where the transfer of data would compromise another individual's rights, WYA will arrange to talk to the individual as soon as possible to discuss the situation, and, if necessary, WYA will take external advice as a matter of priority and, in this situation WYA may need to extend the period before the action is taken.
5. The Right to object
    - Where an individual has an objection to us holding/processing their personal data WYA will ask them to send their objections in writing.
    - WYA will then consider restricting processing until the objection is resolved (see below).
    - WYA will review the lawful reason for holding the data, where it is stored and how it is being used.
    - WYA will consider whether the client's objection outweighs the charity's reason for holding data (note where it is legitimately held, the clients' rights must be considered the more important).
    - WYA will talk to the client about their reasons for holding the data and, if necessary take external advice to resolve the objection.
6. The Right to restrict processing
    - Where an individual objects to their data being held/processed or the charity is not in agreement of other requests they may have made, it may be good practice to restrict processing. An individual can request this too.
    - During this period data may not be used to contact the individual or carry out any work on their behalf.
    - Once the situation has been resolved, the data will be reinstated or erased, depending on the outcome, within one month.
7. The Right to erasure/to be forgotten
    - When someone asks WYA to delete the personal data they hold on them, WYA will ask them to send their request in writing.
    - WYA may ask for ID to prove they are the individual.
    - WYA will consider whether it is appropriate to delete that information. As much of the information is held for purposes, other than consent, there may be good reasons that override the right of the individual.
    - Should there be no objections to actioning the request, WYA will ensure the individual's data is deleted within one month of the request.
    - WYA will review all their files, email accounts etc, to ensure they delete all mentions of it.

Managing requests

- Where a right has been exercised by an individual, as part of the first step consideration should be taken to decide whether it is appropriate to action it.
- Where it is decided that the purposes of processing data outweighs the rights of the individual, Sarah Lawton, as Data Protection Officer, will have the final decision.
- If it is unclear, external advice should be taken before responding to the individual.
- If the response is going to take more than one month, the individual should be communicated with to advise that the request is being investigated and the reason why, and also to advise they will receive a response as soon as possible.

Managing data breaches

A data breach is any access or use of personal data by someone who is not authorised. It could include a mobile device being stolen and accessed or someone inappropriately sharing information from WYA.

- When a breach is identified to have occurred, the Data Protection Officer should be advised and they investigate to determine the impact of the breach.
- If there is considered to be no impact from the breach, the breach should be recorded along with any action taken to rectify and ensure it does not recur.
- In such cases, consideration will be taken as to whether to tighten security, amend procedures or give training. In extreme cases, disciplinary action may be required.
- If there is an impact of the breach, the Data Protection Officer should inform the ICO within 72 hours of the breach being reported and any actions will be taken as advised by them.
- The individuals affected by the breach should also be contacted to advise of the breach and to give any advice, if there's any measures they should take to protect themselves.

Marketing

- Marketing is carried out primarily via Social Media where an individual has a right to control their advertising and where the advertising is done under the GDPR rules of the social media platform.
- Any photos that are used in social media should only be done so with the consent of the individual, or their parent if they are under 18 years old.

HR

- All new staff should be asked to read the GDPR Policy and Procedures and to sign to confirm that they've read them and understood them.
- Staff should be asked to re-read the procedures on a bi-annual basis and to confirm that they have done so and are complying.
- Staff files are kept in BreatheHR as set out on the Data Review spreadsheet and are only accessible by the Chairwoman, Office Manager and HR Trustee.

Volunteers

- Where volunteers have access to personal data that has been supplied to WYA, they will be asked to read the procedures for managing such data and to sign a confidentiality agreement confirming that they understand and agree to use data within the guidelines.
- Where it is believed that a volunteer is using data outside of the guidelines, their access to the data will be removed and they could be asked to stop volunteering for the charity. The 'data breach' procedure may be invoked depending on the use.

Reporting concerns

- Concern or complaints regarding the way information is being handled should be directed to the Data Protection Officer at sarah@simplyoperations.co.uk in the first instance.