Data Protection Policy

Contents

1. Introduction

Whoopsadaisy needs to gather and use certain information about individuals. These can include children and families, suppliers, charity contacts, employees, volunteers, donors, supporters and grant-makers, and other people the charity has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, and stored to meet the charity's data protection standards and to comply with the law.

The UK General Data Protection Regulation and the Data Protection Act 2018 cover all personal data processed by Whoopsadaisy, irrespective of where the data is held and what format it is held in.

Registered with the Information Commissioner's Office: ZB680401

1.1 Why this policy exists?

This data protection policy ensures that Whoopsadaisy:

- Complies with data protection law and follows good practice
- Protects the rights of staff, children and families and other contacts of Whoopsadaisy
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach.

2. Glossary

The following terms are used within the Data Protection Policy and the guidance documents:

- The UK GDPR – UK General Data Protection Regulation
- The DPA – Data Protection Act 2018
- Personal Data – Current data protection legislation applies only to personal data about a living, identifiable individual.
- Special Categories of Personal Data – Personal data is classed as belonging to 'special categories' under current data protection legislation if it includes any of the following types of information about an identifiable, living individual:
    - racial or ethnic origin
    - political opinions
    - religious beliefs
    - union membership
    - physical or mental health
    - sexual life or sexual orientation
    - commission of offences or alleged offences
    - genetic data
    - biometric data.
- Data Subject – A data subject is an individual who is the subject of personal data.
- Processing – Data processing is any action taken with personal data. This includes the collection, use, disclosure, destruction and holding of data.
- Data Controller – A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage, and deletion of the data.
- Data Processor – A data processor is an organisation that processes personal data on behalf of another organisation.

3. Key Considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do you really need to use the information?
- Could anonymised or pseudonymised data be used?
- Do you have a valid justification for processing the data i.e. it is required for a contract or has the data subject given their consent.
- Has the data subject been told about the processing i.e. been issued with a privacy notice?
- Are you sure that the personal data will be secure during the process?
- Are you planning to pass personal data on to a third party? If so, do you have the necessary safeguards/permissions in place to do this?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

4. Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, Whoopsadaisy is required to provide data subjects with a privacy notice to let them know what we are doing with their personal data.

A privacy notice must be:

- easily accessible,
- provided at the time of collecting the data,
- written in a clear and concise way.

4.1 Providing information

Whoopsadaisy aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights.

5. Lawfulness

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) is underpinned by seven important principles. They are intended to provide a comprehensive package to protect personal data. The Act describes how organisations, including Whoopsadaisy, must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To

comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
These say data must:

- Be processed fairly and lawfully,
- Be obtained only for specific, lawful purposes,
- Be adequate, relevant and not excessive,
- Be accurate and kept up to date,
- Not be held for any longer than necessary,
- Processed in accordance with the rights of data subjects,
- Be protected in appropriate ways.

6. Data Sharing

The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees can request it from the manager.
Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within Whoopsadaisy or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their manager if they are unsure about any aspect of data protection.

7. People, risks and responsibilities

This policy applies to all Whoopsadaisy staff and volunteers, suppliers, supporters and grant-makers and other people working with or on the behalf of the charity.
It applies to all data that Whoopsadaisy holds relating to identifiable individuals.
This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Medical information relating to children who are attending sessions at Whoopsadaisy
- Plus, any other information relating to individuals.

7.1 Data protection Risks

This policy helps to protect Whoopsadaisy from some data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how Whoopsadaisy uses data relating to them.
- Reputational damage. For instance, Whoopsadaisy could suffer if hackers successfully gained access to sensitive data.

7.2 Responsibilities

Everyone who works for or with Whoopsadaisy has some responsibility for ensuring data is collected, stored and handled appropriately. Anyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
All data collected by us is to support the service that we deliver to the children who attend Whoopsadaisy.
Specific areas of responsibility are:

- The trustees are ultimately responsible for ensuring that Whoopsadaisy meets its legal obligations.
- The manager, Shonge Holdgate, (01273 554178, shonge@whoopsadaisy.org) is responsible for:
    - Keeping the trustees updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies.
    - Arranging for any data protection training and advice to the people covered by this policy.
    - Handling data protection questions from staff and anyone covered by this policy.
    - Dealing with requests from individuals to see the data Whoopsadaisy holds about them.
    - Checking and approving any contracts or agreements with third parties that may handle Whoopsadaisy's sensitive data.
    - Ensuring all systems and equipment used for storing data meet acceptable security standards.

8. How Personal Data is collected

All personal data is obtained by request by a member of staff. The following covers data that is collected:

- When families first contact Whoopsadaisy they are asked for a phone number and email address.
- When a child is assessed for a place at Whoopsadaisy an assessment form is completed which records any medical history and details on what was observed in the assessment session.

- When offered a place at Whoopsadaisy the parents/carers of the child are asked to complete a registration pack with two consent forms included covering their preferences on how we may use and share any information on the family.
- Staff contact details and an emergency contact phone number are kept. Any references and DBS checks obtained as part of the recruitment process and records of any appraisals that have been completed are also kept.
- Any formal complaints and notes taken from related meetings
- Volunteer contact details are kept along with their application form and any references, and their DBS number and date obtained.
- Contact details and any contracts we may have with chosen suppliers.

9. Data Storage

Described below is how and where data should be safely stored:

- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, these should be locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.
- Data should never be saved directly to mobile devices such as tablets or smart phones.
- All computers containing data should be protected by approved security software and a firewall.

9.1 Photography

Whenever individuals can be identified by their image, data protection legislation applies. In these situations, the rights of the individuals in the collection and use of their photographs must be respected – they must be informed when an identifiable image of them will be or has been captured, and a legal basis must be found before the image is used in any way.

- Photographs of individuals and posed groups: When taking photographs of a specific person that you might want to publish on the internet, you can use ‘legitimate interest’,

‘consent’ and ‘contractual obligation’ as your legal basis. Remember that consent can be withdrawn at any time, and you will have to react accordingly.

- Photographs of crowds: If crowd shots are taken during an event and an individual is not identifiable, then it is not necessary to have a legal basis to take, display or publish the photo. This applies to any individuals, children, and staff whose images are incidental detail, such as in crowd scenes for graduation, conferences and in general event scenes. If the photos are taken at an event where it is likely that individuals may be identified even in crowd scenes, then your legal basis is ‘legitimate interest’. You must, however, include notices at the event informing attendees of the fact that photos are being taken so they have the opportunity to opt out.
- Photographs of children: If taking photographs of children, you must obtain consent from a parent or guardian. This may be written or verbal depending on the circumstances.

10. Data Use

Personal data is of no value to Whoopsadaisy unless the charity can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when unattended.
- Personal data should not be shared informally. It should never be sent by email, or text (mobile phone) as this form of communication is not secure.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

11. Data Accuracy

The law requires Whoopsadaisy to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate the greater the effort Whoopsadaisy should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.
- Whoopsadaisy will make it easy for data subjects to update the information that Whoopsadaisy holds about them.
- Data should be updated as inaccuracies are discovered.
- All digital Data should be kept on OneDrive only and in the correct folders

12. Subject Access Requests

All individuals who are the subject of personal data held by Whoopsadaisy are entitled to:

- Ask what information the charity holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the charity is meeting its data protection obligations.
- Have any data kept on them to be deleted.
- Determine who the data is shared with.
- Decide on the limits of the processing the data.
- Make a complaint to the Information Commissioner's Office – helpline contact number: 0303 123 1113

If an individual contacts Whoopsadaisy requesting information on what data is being held, this is called a subject access request. Subject access requests from individuals should be made by email to shonge@whoopsdaisy.org. Whoopsadaisy will aim to provide the relevant data within 14 days. The identity of anyone making a subject access request will be verified before handing over any information.

12.1 Retention of data

Neither the Data Protection Act nor GDPR specifies time limits for retention of data. The emphasis is on the data controller to identify for how long the data should be retained.
Whoopsadaisy works on the principle that data should 'not be kept longer than necessary for the purpose for which it was processed'.
For data relating to families and children no information will be retained after the child has left the service unless the parents/carers request information is kept and the reason why Whoopsadaisy should keep the information, or the principle above applies.
For staff records the following will apply:

- **Accident Records:** Minimum of 3 years since the last entry, or if it involves a child until they reach 21.
- **Income Tax and NI:** Minimum of 3 years from the end of the financial year to which they relate.
- **Maternity and Paternity:** Minimum of 3 years from the end of the tax year in which the leave ends.
- **Salary and Pay:** Minimum of 6 years.
- **Working Time:** 2 years.

12.2 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed without the consent of the data subject. Under these circumstances Whoopsadaisy will disclose

requested data. However, the legitimacy of the request will be verified, seeking assistance from the trustees and legal advisers where necessary.

13. Data Protection Breaches

Whoopsadaisy is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction, or damage of the data. Whoopsadaisy makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions.
Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of the Whoopsadaisy's Executive Manager (Shonge Holdgate) who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, Whoopsadaisy is required to notify the Information Commissioner's Office as soon as possible, and no later than 72 hours after becoming aware of it. Any member of Whoopsadaisy's community who encounters something they believe may be a data protection incident must email the Executive Manager (Shonge Holdgate) immediately at shonge@whoopsadaisy.org with 'BREACH' in the subject line.

13.1 How to recognise a potential data protection breach

Data protection law defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.
Incidents resulting in the temporary loss or unavailability of personal data may still constitute a personal data breach.
Personal data is information about a living, identifiable individual.
All individuals who access, use, or manage Whoopsadaisy's information are responsible for following these guidelines and for reporting any data protection incidents that come to their attention.

13.2 How to report a potential data protection breach

It is the responsibility of any member of staff who discovers a personal data incident to report it immediately by email to the Executive Manager (Shonge Holdgate) at shonge@whoopsadaisy.org. The email subject line should state 'BREACH'.
Staff members who report a data protection breach will be asked to complete Part A of the Data Protection Breach Response Evaluation Form within 24 hours of discovering the potential breach involving personal data.

13.3 Data Protection Breach Response Evaluation Form

Data Protection Breach Response Evaluation Form

Please ensure Part A of this form is completed and returned as soon as possible and certainly within 24 hours of discovering the potential breach involving personal data.

Whoopsadaisy is required by data protection law to report certain types of personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach if it is likely to result in adverse effects on individuals' rights and freedoms. Where there is a likely high risk of these adverse effects occurring, Whoopsadaisy is also required to notify the individuals without delay.
As the information provided in this form will be used to assess the likelihood and level of risk to individuals, you must complete the form to the best of your ability.

PART A: GATHERING THE FACTS

To be completed by the person reporting the data protection breach

Employee details	
Name	
Position	
Phone number	
Email	
Incident details	
Date and time of data breach	
Location of data breach	
How was the breach detected?	
Description of incident	Select/highlight the option that fits most closely: • Misdirected communication (e.g. sending an email or letter to the wrong recipients) • Mislaid data (e.g. leaving a paper file or portable device in a public place) • Theft of device/hardware containing data • Premature destruction or deletion of golden copy data contrary to the retention schedule

	• Unauthorised access to data (e.g. through hacking, phishing etc) • Unauthorised editing/amendment of data (e.g. by a disgruntled employee) • Other: please specify
Data subjects	Select/highlight all categories that apply: • Children • Staff • Volunteers • Applicants • Other: please specify

Format of data	Select/highlight all categories that apply:
	• Paper
	• Email with or without an attachment
	• Digital data on a removable/portable device:
	  ○ Whoopsadaisy owned laptop
	  ○ Personally owned laptop
	  ○ Whoopsadaisy owned smart phone
	  ○ Personally owned smart phone
	  ○ USB drive
	• Digital data on OneDrive
	• Digital data on third party server / cloud
	• Other: please specify

Categories of personal data	Select/highlight all categories that apply:
	• Personal identifiers
	  ○ Name
	  ○ Date of birth
	  ○ Other: please specify
	• Contact details
	  ○ Home address
	  ○ Home/personal telephone number
	  ○ Home/personal email address
	  ○ Work address
	  ○ Work telephone number
	  ○ Work email address
	  ○ Other: please specify
	• Financial information
	  ○ Bank details
	  ○ Salary information
	  ○ Other: please specify
	• Progression information
	  ○ Notes / goals / Progress reports
	  ○ Appraisal / annual review information
	  ○ Other: please specify
	• Criminal convictions or offences
	• Special Category personal data
	  ○ Health (e.g. sickness absence information, including medical certificates; Special circumstances information; Disability information; medical records)
	  ○ Genetic or biometric data
	• Other: please specify

Number of individuals/personal data records	

In addition to the personal data is any other information involved?	
Actions taken	
What actions have been taken so far in response to the incident? If relevant, what is being done to recover the information and/or prevent the further transmission of the information and/or delete the information mistakenly disclosed?	(E.g. If information was sent electronically to an incorrect recipient(s), have they been asked to delete the information? If a device was lost or stolen and remote wipe is possible, has this been done? If a password has been disclosed, has it been changed?)
If applicable: what action was taken by the recipient when they inadvertently received the information?	
Have you already notified the data subjects?	(If so, explain how and attach correspondence)

PART B: INITIAL ASSESSMENT

To be completed by the Executive Manager

When assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. A risk exists when the breach may lead to physical, material, or non-material damage for the individuals whose data have been breached. Where the breach involves special category personal data, criminal convictions and offences or related security measures, such damage should be considered likely to occur.

Taking into account the following issues, assess the likelihood and severity of the risk:

- Type of breach
- The nature, sensitivity, and volume of personal data
- Ease of identification of individuals
- Severity of consequences for individuals
- Special characteristics of the individual
- Special characteristics of Whoopsadaisy
- The number of affected individuals

Risk	Assessment of Likelihood and Severity
Discrimination	
Loss of control by data subject over their personal data	
Limitation of the data subjects' rights	
Identity theft or fraud	
Financial loss	
Damage to data subjects' reputation	
Loss of confidentiality of personal data	

Other: please specify	

Based on the above assessment, decide the categorisation of the breach.

Decision	
Breach Categorisation and Assignment	Breach notifiable or unlikely to be notifiable
Explain the reason for the categorisation	

PART C: ACTIONS TAKEN AFTER BREACH REPORTED

To be completed by the Executive Manager

Action	
Breach notified to the ICO?	Yes/No, explain justification for decision
Data subjects notified?	Yes/No, explain justification for decision
Further actions taken as a response?	
Actions taken to prevent similar incident?	
If the breach was notified to the ICO, what was the outcome?	
If data subjects were notified about the breach, what was the outcome?	

Policy reviewed: 23 April 2024.

Approved: ……

Chair of Trustees