Data Protection Policy incorporating GDPR.

Policy and Procedures.

1. Introduction

1.1. Wildside Activity Centre is committed to a policy of protecting the rights and privacy of individuals. The Centre needs to collect and use certain types of Data in order to carry on its work. This personal information must be collected and dealt with appropriately.

1.2. The Data Protection Act 2018 governs the use of information about people (personal data). Personal data can be held on computer or in a manual file, and includes emails, minutes of meetings, and photographs. Wildside Activity Centre will remain the data controller for the information held. Wildside staff and volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act. Board members who have access to personal information are also expected to read and comply with this policy.

1.3. As a matter of good practice, if other organisations and individuals working with the Centre have access to personal information, they will be expected to comply with this policy and complete appropriate agreements for data exchange. It is expected that where any staff have to share information with external organisations, with the approval of the Data Protection Officer, they will take responsibility for ensuring that such organisations complete such an agreement.

2. Purpose

2.1. The purpose of this policy is to set out the commitment of Wildside Activity Centre and its procedures for protecting personal data. The Board regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. Wildside Activity Centre (Wildside) is committed to a policy of protecting the rights and privacy of all persons involved directly or indirectly with the Centre.

3. The Data Protection Act Legislation 2018

3.1. The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). GDPR was introduced on 25 May 2018, standardising European data protection rules across all member states. If the UK leaves the European Union, GDPR will continue to apply to the UK, as it will be incorporated in the European Union (Withdrawal) Agreement.

3.2. New requirements would apply to the transfer of personal data to or from countries in the EU but since Wildside deals only with a UK market, this does not currently affect the Centre's work. If the UK remains a part of the EU, GDPR will also continue.

3.3. The Data Protection Act 2018 contains 8 principles for processing personal data with which Wildside Activity Centre will comply.

3.4. **Personal data**

3.4.1 Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

3.4.2 Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,

3.4.3 Shall be adequate, relevant and not excessive in relation to those purpose(s),

3.4.4 Shall be accurate and, where necessary, kept up to date,

3.4.5 Shall not be kept for longer than is necessary

3.4.6 Shall be processed in accordance with the rights of data subjects under the Act

3.4.7 Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

3.4.8 Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

4. Definitions

4.1. Definitions used by Wildside are drawn from the GDPR (Material scope, Article 2). GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

4.2. **The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:**

4.2.1 Data Controller – The person who (either alone or with others) decides what personal information is to be collected and how it will be held or used.

4.2.2 Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

4.2.3 Data Protection Officer – The person who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998

4.2.4 Data Subject/Service User – The individual whose personal information is being held or processed (for example: a service user or a supporter)

4.2.5 ‘Explicit’ consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

4.3. Explicit consent is needed for processing sensitive data: this includes the following:

4.3.1 racial or ethnic origin of the data subject
4.3.2 political opinions
4.3.3 religious beliefs or other beliefs of a similar nature
4.3.4 trade union membership
4.3.5 physical or mental health or condition
4.3.6 sexual orientation
4.3.7 criminal record
4.3.8 proceedings for any offence committed or alleged to have been committed

4.4. **Notification** – Notifying the Information Commissioner's Office (ICO) about the data processing activities of the Centre, as applicable.

4.5. **Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

4.6. **Processing** – means collecting, amending, handling, storing or disclosing personal information.

4.7. **Personal Information** – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses, an identification number, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that person, including pictures. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual users.

5. Policy statement

5.1. The GDPR and this policy apply to all of Wildside's personal data processing functions, including those performed on customers', users', clients', employees', suppliers' and partners' personal data, and any other personal data Wildside processes from any source.

5.2. The Data Protection Officer/GDPR Owner is responsible for reviewing the register of processing annually in the light of any changes to Wildside's activities and for carrying out any additional requirements identified by means of data protection impact assessments (DPIA). This register needs to be available on the request of the Information Commissioner's Office (the supervisory authority). The DPIA is used to capture and review all data processing.

5.3. This policy applies to all Employees/Staff [and interested parties] of Wildside such as outsourced suppliers. Any breach of the GDPR will be dealt with under Wildside's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

5.4. Partners and any third parties working with or for Wildside, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

5.5. No third party may access personal data held by Wildside without having first entered into a data sharing or data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Wildside is committed.

6. Responsibilities and roles under the General Data Protection Regulation

6.1. Wildside is the *data controller* under the GDPR. Managers and all those in managerial or supervisory roles throughout Wildside are responsible for developing and encouraging good information handling practices within Wildside; the Data Protection Officer/GDPR Owner, a role specified in the GDPR, is a member of the senior management team, who is responsible for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

6.2. Development and implementation of the GDPR as required by this policy;

6.3. Security and risk management in relation to compliance with the policy;

6.4. The Business Development Manager has been appointed by the Board as *Data Protection Officer* and GDPR Owner for Wildside and has been given responsibility for Wildside's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Wildside complies with the GDPR. Wildside is registered with the Information Commissioner's Office, which monitors data protection issues and uphold information rights in the public interest.

The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance. Compliance with data protection legislation is the responsibility of all employees of Wildside who process personal data. Employees of Wildside are responsible for ensuring that any personal data about them and supplied by them to Wildside is accurate and up-to-date.

7. Data protection principles at Wildside

7.1. All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Wildside's policies and procedures are designed to ensure compliance with the principles. Personal data must be processed lawfully, fairly and transparently.

7.1.1 Lawful: identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

7.1.2 Fairly: in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

7.1.3 Transparently**:** the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

7.2. The specific information that Wildside will provide to the data subject must, as a minimum, include:

7.2.1 The identity and the contact details of the controller and, if any, of the controller's representative;

7.2.2 The contact details of the Data Protection Officer;

7.2.3 The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

7.2.4 The period for which the personal data will be stored;

7.2.5 The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

7.2.6 The categories of personal data concerned;

7.2.7 The recipients or categories of recipients of the personal data, where applicable;

7.2.8 Any further information necessary to guarantee fair processing.

7.3. This is covered by the Wildside privacy statement on the website and the statements on the booking forms.

7.4. The Data Protection Officer/GDPR Owner is responsible for ensuring that Wildside does not collect information that is not strictly necessary for the purpose for which it is obtained.

7.4.1 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to a privacy statement and be approved by the Data Protection Officer.

7.4.2 The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed by resource owners to ensure that collected data continues to be adequate, relevant and not excessive. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

7.4.3 Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

7.4.4 It is also the responsibility of the data subject to ensure that data held by Wildside is accurate and up to date.

7.5. Employees/Staff are required to notify Wildside of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Wildside to ensure that any notification regarding change of circumstances is recorded and acted upon.

7.6. The Data Protection Officer / GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

7.7. On at least an annual basis, the Data Protection Officer / GDPR Owner will review the retention dates of all the personal data processed by Wildside, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted or destroyed.

7.8. The Data Protection Officer / GDPR Owner is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If Wildside decides not to comply with the request, the Data Protection Officer / GDPR Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

7.9. The Data Protection Officer / GDPR Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, they are informed that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

7.10. Personal data will be retained in line with the Retention and Disposal Schedule and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

7.11. The Data Protection Officer / GDPR Owner must specifically approve any data retention that exceeds the retention periods defined in the Retention and Disposal Schedule, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written and filed.

7.12. Personal data must be processed in a manner that ensures appropriate security. The Data Protection Officer / GDPR Owner will carry out a risk assessment taking into account all the circumstances of Wildside's controlling or processing operations. In determining appropriateness, the Data Protection Officer / GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Wildside itself, and any likely reputational damage including the possible loss of customer trust.

7.13. When assessing appropriate IT technical measures, the Data Protection Officer / GDPR Owner will consider the following:

7.13.1 Password protection

7.13.2 Virus checking software and firewalls

7.13.3 Encryption of devices that leave the organisation's premises such as laptops

7.13.4 Security of local and wide area networks.

7.14. When assessing appropriate organisational measures, the Data Protection Officer / GDPR Owner will consider the following:

7.14.1 The appropriate training levels throughout Wildside;

7.14.2 Measures that consider the reliability of employees (such as references etc.);

7.14.3 The inclusion of data protection in employment contracts;

7.14.4 Identification of disciplinary action measures for data breaches;

7.14.5 Monitoring of staff for compliance with relevant security training completion;

7.14.5 Physical access controls to electronic and paper based records;

7.14.6 Storing of paper based data in lockable cabinets;

7.14.7 Restricting the use of portable electronic devices outside of the workplace;

7.14.8 Adopting clear rules about passwords;

7.14.9 Making regular backups of personal data and storing the media off-site

7.14.10 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

7.15. Wildside has complied with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical

and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident management response plans.

8. Data subjects' rights

8.1. Data subjects have the following rights regarding data processing, and the data that is recorded about them:

8.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.
8.1.2 To prevent processing likely to cause damage or distress.
8.1.3 To prevent processing for purposes of direct marketing.
8.1.4 To be informed about the mechanics of automated decision-taking processes that will significantly affect them.
8.1.5 To have no significant decisions that will affect them taken solely by automated process.
8.1.6 To request compensation if they suffer damage by any contravention of the GDPR.
8.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
8.1.8 To request the Information Commissioner's Office to assess whether any provision of the GDPR has been contravened.
8.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
8.1.10 To object to any automated profiling that is occurring without consent.
8.1.11 Data subjects have the right to complain to Wildside related to the processing of their personal data, the handling of a request for data and appeals.

9. Consent

9.1. Wildside understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

9.2. Wildside also understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them.

9.3. There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that consent was obtained for the processing operation. For sensitive data, explicit consent of data subjects must be obtained unless an alternative legitimate basis for processing exists. In most instances, consent to process personal and sensitive data is obtained routinely by Wildside using standard consent documents such as a booking form for an activity or a membership form. This requirement also applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

10. Security of data

10.1. All Employees/Staff are responsible for ensuring that any personal data that Wildside holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Wildside to receive that information and has entered into a confidentiality or data sharing agreement.

10.2. All personal data should be accessible only to those who need to use it and should be treated with the highest security and must be kept:

10.2.1 In a lockable room with controlled access; and/or

10.2.2 In a locked drawer or filing cabinet; and/or

10.2.3 If computerised, password protected.

10.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Wildside. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation.

10.4. Personal data may only be deleted or disposed of in line with the Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as ‘confidential waste’. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

10.5. Staff must be specifically authorised to process data off- site and such permission will not normally be given.

10.6. All Wildside's computers should have a log in system and passwords should be used for protection of data where appropriate. All personal data is kept in a locked cabinet. Staff members should not take personal data out of the office on laptops or memory sticks and care should always be taken to ensure that personal data on screen or on paper is not visible to strangers.

11. Disclosure of data

11.1. Wildside will ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees and Staff will exercise caution when asked to disclose personal data held on another individual to a third party. All requests to provide data for one of these reasons will be supported by appropriate paperwork and all such disclosures will be specifically authorised by the Data Protection Officer / GDPR Owner.

12. Retention and disposal of data

12.1. Wildside shall not keep personal data in a form that permits identification of data subjects for a period longer than is necessary, in relation to the purpose(s) for which the data was originally collected.

12.2. Wildside may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

12.3. Personal data will be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

13. Data transfers

13.1. All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

13.2. Wildside will not transfer data to any 3rd party outside the EEA.

14. Information asset register/data inventory

14.1. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by Wildside, and in relation to processing undertaken by other organisations on behalf of Wildside.

14.2 Wildside shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

14.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of individuals, Wildside shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

14.4 Where, as a result of a DPIA it is clear that Wildside is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Wildside may proceed must be escalated for review to the Data Protection Officer/GDPR Owner.

14.5 The Data Protection Officer / GDPR Owner shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Wildside Board of Directors.

14.6 Appropriate controls will be selected and applied to reduce the level of risk associate with processing individual data to an acceptable level, by reference to Wildside's documented risk criteria and the requirements of the GDPR.