DATA PROTECTION POLICY

1. Introduction:

This policy outlines the framework of how Wings South West staff must handle personal data to ensure compliance with UK GDPR. Although Wings South West has not-for-profit organisation status and our usage of information is limited, the Information Commissioner's Office has been notified due to the use of CCTV cameras.

2. Scope:

This policy applies to the processing of personal data which is defined by article 4 of the UK GDPR. This policy applies to all Wings staff, Sessional workers, Trustees and Volunteers who have access to information used for Wings purposes.

Where this policy reads "staff", it should be read to include all those mentioned above.

3. Breach of this Policy:

All reckless or deliberate breaches of this policy will be investigated and may be referred to the Board of Trustees, who with management will consider whether disciplinary action should be taken against the member of staff concerned. Alleged breaches will also be investigated by the Data Protection Officer (DPO- Andy Best) and can be referred onto management and the Trustees as considered necessary.

4. Policy Review:

This policy will be reviewed by the DPO every 3 years and approved by the board of Trustees.

5. Responsibilities:

Responsibility for UK GDPR compliance rests with the Board of Trustees/CEO and the DPO. The Data Protection Policy is managed, maintained and communicated to staff by the DPO.

6. The data protection principles:

The UK GDPR is underpinned by six common-sense principles that govern the way in which Wings South West must process personal data. These principles are outlined in article 5 of the UK GDPR and are summarised below:

- *Personal data shall be processed lawfully, fairly and in a transparent manner.*
- *Personal data shall be collected for specified, explicit and legitimate purposes.*
- *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*
- *Personal data shall be accurate and, where necessary, kept up to date.*
- *Personal data shall be kept no longer than necessary.*
- *Personal data shall be processed in a manner that ensures its security.*

Personal data covers facts, opinions and images about the individual. It also includes information regarding the intentions of the data controller (the person who controls the use of data and processing methods used) towards the individual; although in some limited

circumstances exemptions will apply. With processing, the definition is far wider than before, for example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'.

7. Consent:

If Wings South West is required to obtain consent, we will ensure that the following requirements are met;

- The consent is freely given.
- The person giving the consent understands fully what they are consenting to.
- The person giving consent must be either aged over 18 years old or be signed for by a parent/legal guardian. Those with disabilities, legal guardians/parents will determine if they are able to sign their own consent if over 18 years of age.
- There must be a positive indication of consent (Opt-in as opposed to opt-out)
- The person giving consent must be able to withdraw their consent at any time.
- Consent should be documented so that it may be referred to in the future, if necessary.

(However, regarding the courses that are run at Wings South West, data of individuals is a prerequisite for attending courses and those refusing to give the information could find they cannot attend a course for example, Staff require medical information and emergency contact information at a minimum for safety.)

8. Rights of data subjects:

Article 3 of the UK GDPR outlines the rights afforded to individuals in respect of the processing of their personal data. These are summarised below:

- The right to transparency of the processing of their personal data
- The right to access
- The right to rectification
- The right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object to processing
- The right to request human intervention if processing is by automated means

Requests to manage these rights are managed by the DPO. Any amendments to consent or data can be made by completing a new Personal Information Form and handing it into a member of Staff. To erase data from Wings South West, subjects should complete FORM DP1, Access to Subject Data for Erasure.

9. Security Incident management and notification:

An information security incident (ISI) can occur when the confidentiality, availability and or integrity of personal data is put at risk. Examples of activities considered an ISI might include; information being at risk of being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of Wings South West; sold or used without the permission of Wings South West or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

Wings South West has a Security Incident Management Procedure (SIMP) appendix 1 in place which governs how Wings and its staff must report and handle incidents. This procedure must be followed at all times.

An information security incident can compromise business operations resulting in embarrassment to Wings South West or loss of trust in the organisation, by clients or members of the public. Information security incidents involving personal data can also result in a breach of the General Data Protection Regulation (UK GDPR) and other relevant data protection laws, which can lead to Wings South West being fined up to £17.5 million or 4% of our turnover by the Information Commissioners Office. Such breaches can also adversely affect someone's privacy causing them damage and/or distress, which can lead to successful law suits as a result. Wings South West therefore takes all security incidents very seriously.

Every ISI must be reported to the DPO. See the SIMP (Appendix 1) for how to report an incident.

If you suspect a Staff member (section 2.) is accessing or disclosing personal data or sensitive business data inappropriately, you must also report this to the DPO; your manager or the CEO immediately.

Staff will be given the appropriate procedures to follow when handling personal data.

In accordance with article 39 of the UK GDPR, Wings South West is committed to notifying the Information Commissioner's Office or relevant supervisory authority within 72 hours, of being notified of a breach that might adversely affect the rights and freedoms of a data subject. Notifications of this nature are the responsibility of the DPO.

10. The Data Protection Officer (DPO):

Article 37 of the UK GDPR requires that Wings South West appoints a DPO to undertake the tasks outlined in article 39 of the UK GDPR. Contact details for the DPO will be made publicly available and will be referred to in all privacy notices.

Wings South West will commit to ensure that the DPO is sufficiently resourced to undertake the tasks assigned to them under article 39 of the UK GDPR. Wings South West will also ensure that the DPO is consulted on all matters which concern the processing of personal data.

The DPO will liaise with the CEO regarding any contact with the Information Commissioner's Office or other relevant supervisory authorities.

11. Transfers outside the UK:

Wings South West will not transfer any personal data to countries outside of the UK unless one or more of the following qualifying criteria are met;

- An adequate decision has been made in accordance with article 45 of the UK GDPR
- The transfer is the subject of appropriate safeguards in accordance with article 46 of the UK GDPR
- The transfer is the subject of binding corporate rules in accordance with article 47 of the UK GDPR

- If one or more of the special circumstances outlines in article 49 of the UK GDPR are met.

12. Use of Images of People - Photographs, Videos, Webcams and Websites

Under the Data Protection Act 2018;

- Written or recordable permission must be obtained from all the people, or their parents/guardians who will appear in a photograph, video or webcam image to be used for publicity purposes, before the image is published (use the Personal Information Form, PIF).
- This includes children as well as adults: if the image is of children under 16, the parent's permission must be obtained (use PIF).
- The reason the person's image is being used, what it will be used for, and who might want to look at the pictures is made explicit on the PIF.

If images are being taken at an event attended by large crowds, such as a sports event, this is regarded as a public area so permission is not needed from everyone in a crowd shot. People in the foreground are also considered to be in the public area so their consent is not needed.

However, if an image of, for example, the winner of a race at a sports event is to be used - with the crowd in the background - the race winner's, or their parents', verbal permission must be obtained and then recorded. Their consent can be recorded when the photograph is taken or any time after, prior to publication.

For Child Protection purposes, on no occasion should written details of children and young people under the age of 18 ever be contained or published in any literature or websites. These details include identification by first and/or surname, e-mail or postal addresses, telephone numbers and tags on social media (we do state the group, e.g. Unity or NDCA for publicity purposes on social media with permission from the individuals)

When using photographs of young people, group pictures will be preferred to individual images, especially where an event can be located to a 'small' unit, eg a local school.

A list of young people for whom permission to use photographs has been refused will be kept and regularly updated. Where permission is refused, a letter will be sent to the parent/guardian to inform them that the organisation cannot be responsible for photographs taken by other young people or visiting adults (e.g. at a performance)

13. Requests by Individuals to View CCTV Images

Requesting CCTV information should be done by using the Subject Access Request Form DP2b, which includes stating the reason why a data subject is wishing to view the images. Subsequent disclosure will be authorised by the DPO subject to confirmation from the Operations Manager, CEO or a Trustee.

14. Ensuring security of personal data throughout the organisation

14.1 Computer Security:

- Firewalls, anti-spyware and virus-checking software are installed on all computers and the network.
- The operating system is set up to receive automatic updates.
- Computers are protected by downloading the latest patches or security updates, which should cover vulnerabilities.
- Staff ensure laptops and computers are password protected so that sensitive information cannot be accessed by young people or others.
- Staff have access to the information they need to do their job and do share passwords.
- Regular back-ups of the information on computers and laptops are taken and kept on the server.
- All personal information is removed from old computers before disposal.
- Use of memory sticks is discouraged apart from sharing of photographs. Where needed, an encrypted memory stick will be issued.

14.2 Other security:

- The buildings are physically secure and alarmed.
- Personal information containing the names and other details of young people is stored either
    - In a locked filing cabinet in Lendon Barn.
    - In secure online cloud storage.
- Personal information is never left around in the office or elsewhere. Staff to keep desks clear.
- Young People, volunteers and visitors are never left unaccompanied in the office.
- Access to the online storage is restricted to essential staff.
- Information is published only where consent has been received in accordance with section 12.

14.3 Transporting sensitive information:

- Great care will be taken when transporting personal information, as this is where most losses occur.
- When paperwork is transported from one site to another, it will be kept in a folder and transferred immediately to a secure place.
- Information will not be left in workers' cars or taken home for any reason.
- Laptops may be taken home, but must be password protected, and care must be taken that sensitive information is not seen even by family members.

Signed: ……. …… Dated: ……
CEO

FORM DP2a
DATA ACCESS FORM

The Wings Hall Lower Meddon Street Bideford EX39 2BJ Tel: 01237 472000
Lendon Barn Abbotsham EX39 5BW Tel: 01237 471471
email: admin@wingscharity.com

SUBJECT ACCESS FORM

ACCESS TO SUBJECT DATA FOR ERASURE

(Amendments can be made by completing a new Personal Information Form)

Request made by (name in caps) .....

Address .....

.....

Tel No ..... Mob No .....

I (named subject, IN CAPS) ..... wish to delete my data from Wings South West.

Signed (Named Subject) ..... Date.....

Authorised by Operations Manager/CEO/Trustee* Signed .....

Name (in caps) ..... Date .....

Data Controller's signature .....

Name (in caps) ..... Date .....

* Delete as applicable

FORM DP2b
DATA ACCESS FORM

The Wings Hall Lower Meddon Street Bideford EX39 2BJ Tel: 01237 472000
Lendon Barn Abbotsham EX39 5BW Tel: 01237 471471
email: admin@wingscharity.com

SUBJECT ACCESS FORM

FOR ACCESS TO CCTV IMAGES

Request made by (name in caps) .....

Address .....

.....

Tel No ..... Mob No .....

About the images requested to be accessed

Date of incident .....

Time of incident .....

Reason why requesting to see images .....

.....

.....

PLEASE NOTE: Under the Data Protection Act, Wings personnel are not obliged to release CCTV information.

Were the CCTV images shown to the person requesting above? YES/NO*

Authorised by Operations Manager/CEO/Trustee* Signed .....

Name (in caps) ..... Date .....

Data Controller's signature .....

Name (in caps) ..... Date .....

* Delete as applicable

SECURITY INCIDENT MANAGEMENT PROCEDURE

The intention of this procedure is to ensure that an information security incident (ISI) is reported, monitored and handled appropriately. It is intended that this procedure will help ensure that Wings South West is able to respond to an information security incident appropriately and in a way that lessens the impact on a data subject. This procedure is also in place to help Wings South West, to ensure appropriate learning from incidents takes place, and to ensure that reoccurrences do not happen in future.

Reporting an information or data security incident:
Members of the public and members of staff should report an ISI to the Data Protection Officer as soon as possible. 'Near Misses' must also be reported as it is important that Wings South West is aware of any risks that might expose our information to future incidents.

Those wishing to report an ISI can remain anonymous if they prefer and are therefore not required to provide their name or contact details when reporting an incident. However, this information may be useful when identifying and investigating the ISI. The information provided during the notification of an incident will be treated sensitively and securely, although it may be necessary to share information provided during notification of an incident, with senior managers, and serious incidents, the CEO and or the Board of Trustees.

Logging a security incident:
The Data Protection Officer (DPO) is responsible for overseeing information security incident investigations. Upon being notified of an ISI the DPO will undertake the following actions:

1)Log the Incident on the Wings South West Security Incident Management Spreadsheet within 2 working days of receipt.

2)Acknowledge receipt of an ISI notification (if contact details are left) within 2 working days of receipt.

3)Gather sufficient information to enable a risk assessment to be undertaken within 2 working days of receipt.

4)Carry out an assessment of the severity of the incident within 3 working days of receipt.

5)Notify the Information Commissioner's Office or relevant supervisory authority within 72 hours of becoming aware of an information security incident that might adversely affect the rights and freedoms of a data subject.

Data Incident Classification:

DATA INCIDENT CLASSIFICATION	DESCRIPTION
No Incident	The actions which gave rise to the incident notification have not jeopardised the confidentiality, availability or integrity of Wings South West's information.
No Incident – near miss	There is a risk that the actions which gave rise to the incident notification, might adversely affect the confidentiality, availability or integrity of Wings South West's information. However, this risk has not materialised in this case.
Low Risk Incident	The confidentiality, availability or integrity of Wings South West's information has been adversely affected. However, the impact of this incident on Wings is negligible. If the incident involved personal data, the incident has not impacted adversely on the rights and freedoms of the data subject.
Medium Risk Incident	The confidentiality, availability or integrity of Wings' information has been significantly affected such that there is a measurable impact on the organisation. If the incident involved personal data, the incident has not impacted adversely on the rights and freedoms of the data subject.
High Risk Incident	The confidentiality, availability or integrity of Wings' information has been significantly impacted to such an extent that there are significant business continuity risks, reputational risks or risk or regulatory action. If the incident involved personal data, the incident has caused a negative effect on the rights and freedoms of the data subject.

Data Incident Notification to Key Staff:

High risk incidents will be notified within 2 working days to the Chief Executive, the Wings' Solicitor, the Board of Trustees and the Data Protection Officer.

Medium risk incidents will be notified within 5 working days to Line Manager of the staff responsible and the data protection officer.

Low risk incidents will be notified within 7 working days to the Line manager of staff responsible and the data protection officer.

No incidents and near misses will be notified as soon as possible to the line manager of the person reporting and the data protection officer.

Notifying Data Subjects:

All information security incidents that are likely to negatively impact on the rights or freedoms of a data subject, will be notified about the incident by Wings South West without undue delay. Such notifications will include the following information;

- An apology for the incident which has occurred
- A description of the information put at risk
- A description of any risk that this incident might cause the data subject
- A description of how the incident occurred
- Details of any steps taken by Wings to remedy the incident and prevent a reoccurrence
- Guidance on how the data subject can protect themselves from the effects of the information security incident
- Details of how the data subject can make a formal complaint to Wings and the Information Commissioner's Office.
- Details of who Wings has notified about the incident in question

All notifications above of this procedure will be made verbally over the telephone, in person or in written form. All written notification will be in plain English and will conform to Wings' standards of letter writing.

Review of Information Security Incidents:
The DPO will ensure that the information risks associated with all ISI are recorded, monitored and escalated to the CEO where necessary.

Actions proposed in response to an ISI investigation will be monitored by the DPO and will be reported to the Board of Trustees quarterly.

If improvements identified in an ISI investigation have not been made by particular staff members, and/or if similar security incidents have been reported involving the actions of a particular staff member, the DPO will notify the Line manager of the staff member concerned. The CEO and the Board of Trustees will also be alerted and will decide if disciplinary action is necessary.