



Wyvern Foundation
Registered Charity 1124103
Data Management Policy

Scope of the Policy

Wyvern Foundation needs to gather and use certain information about individuals. These include young people and /or a parent or person holding parental control, 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 word 'applicant' used throughout this document refers to the young person applying for a grant or bursary or the parent or person holding parental control applying on behalf of the young person.

Why this policy exists

This data protection policy ensures that the Wyvern Foundation:

- Complies with data protection law and follows good practice.
- Protects the rights of the committee and applicants.
- Is open about how it stores and processes data.
- Protects itself from the risks of a data breach.

Data Protection Principles

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018 and identifies 8 data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.

Principle 6 - Personal data must be processed in accordance with the individuals' rights.

Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Lawful, fair and transparent data processing

The Wyvern Foundation requests personal information from committee members and applicants for the purpose of sending communications about their involvement with the Foundation. The forms used to request personal information will contain a personal consent section. The Privacy statement can be accessed via the Wyvern theatre Website. Click on About Us and select Wyvern Foundation from the drop-down menu. It is available in hard copy by contacting the Wyvern Foundation c/o the Wyvern Theatre Box Office. Committee members and applicants will be asked to provide consent for their data to be held and a record of this consent will be securely held. Committee members and applicants will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once a committee member or applicant requests not to receive certain communications this will be acted upon promptly and the person will be informed as to when the action has been taken.

Processed for Specified, Explicit and Legitimate Purposes

Committee members and applicants will be informed as to how their information will be used and will be assured that personal data will not be used inappropriately. Appropriate use of information provided will include:

- Communications about the Wyvern Foundation's events and activities
- Communications with applicants about their applications
- Communications about meetings

Inappropriate communication would include sending marketing and/or promotional materials from external service providers.

The Wyvern Foundation will ensure that personal information is managed in such a way as to not infringe an individual's rights which include:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

Adequate, Relevant and Limited Data Processing

Committee members and applicants will only be asked to provide information that is relevant to the charitable activities of the Wyvern Foundation. This will include:

- Name.
- Postal address.
- Email address.
- Telephone number.

Data on committee members will only be kept whilst an individual remains a committee member and will then be deleted/destroyed unless the member expressly opts to remain on the contact list. Applicants' data will be kept for a maximum of two years after their application. All data no longer required will be deleted/shredded and disposed of securely.

Data Sharing

The Foundation receives applications for bursaries for the Summer Youth Project run by The Wyvern Theatre. Applications are passed to two members of the committee for approval. The forms are also subject to our Data Management Policy and Privacy Statement. Any applications for grants or bursaries, when shared, will be anonymised.

Accuracy of Data and Keeping Data up to Date

Committee members and applicants will be advised that they should ensure that the Wyvern Foundation is informed if their personal information changes.

No more than two committee members, including the Chair will have access to the email account. When one of those people leaves the committee, the other member will change the email password. If both leave at the same time, those leaving will pass the existing password on to their successors, who will immediately change it.

General Guidelines for Committee

- The only people able to access data covered by this policy should be those who need to communicate with committee members or provide a service to those applying to the Wyvern Foundation for grants or bursaries.
- The Wyvern Foundation will provide induction training to committee members to help them understand their responsibilities when handling personal data.
- Committee members should keep all data secure by taking sensible precautions and following the guidelines.
- Personal data should not be shared outside of the Wyvern Foundation unless with prior consent and/or for specific and agreed reasons.

Accountability and Governance

The Committee members are responsible for ensuring that the Wyvern Foundation remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance. The Chairperson will ensure that new committee members receive an induction into how data protection is managed within the Wyvern Foundation and the reasons for this. The Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held.

Secure Processing

The Committee of the Wyvern Foundation has a responsibility to ensure that data is both securely held and processed. This will include:

- Restricting access of applicant information to those committee members who need to communicate with applicants.
- Committee members processing data using strong passwords.
- Committee members processing data not sharing passwords.
- Using password protection on laptops, PCs and phones that contain or access personal information.

Subject Access Request

The Wyvern Foundation Committee members and applicants are entitled to request access to the information that is held by the Foundation. The request needs to be received in the form of a written request to the Secretary of the Foundation. There is no charge for this request. On receipt of the request, it will be formally acknowledged and dealt with within one month unless there are exceptional circumstances as to why the request cannot be granted. The Foundation will provide a written response detailing all information held on the applicant. A record will be kept of the date of the request and the date of the response.

Data Breach Notification

Were a data breach to occur, action will be taken to minimise the harm by ensuring all committee members are aware that a breach has taken place and how the breach had occurred. The Committee members shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chairperson of the Foundation will contact, where necessary, the Information Commissioner's Office. The committee will also contact the relevant committee members/applicants to inform them of the data breach and actions taken to resolve the breach.

If the Foundation is contacted to say that a breach may have occurred, that person will be asked to provide an outline of their concerns. If the initial contact is by telephone, the person reporting the suspected breach will be asked to follow this up with an email or a letter detailing their concern. The concern will then be investigated by committee members who are not in any way implicated in the breach. Where the committee member needs support or if the breach is serious the Chairperson should notify Information Commissioner's Office. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: November 2019