Date: 17 January 2017
For: Employees/volunteers, referrers, members

Data Protection Policy

Introduction

The Data Protection Act 1998 requires that anyone processing personal data must comply with the eight principles of good practice. These are that data shall:

- be fairly and lawfully processed;
- be obtained and processed for specified and lawful purposes only;
- be adequate, relevant and not excessive;
- be accurate and where necessary, kept up to date;
- not be kept longer than necessary;
- be processed in accordance with the subject's rights;
- be kept secure;
- not be transferred outside the EU without adequate protection.

Ride High is committed to ensuring that all employees/volunteers and Trustees who have access to any personal data held by Ride High are aware of and abide by their responsibilities under the Data Protection Act.

To comply with the above principles (and therefore to comply with the Act), when collecting data we need to:

(a) be sure we need the information;

(b) know what we are going to use it for;

(c) be sure that the people (or the parent/carer of a child or young person) whose information we hold know that we have it, and are likely to understand what we will use it for;

(d) be satisfied that we only pass on personal information if the people (or the parent/carer of a child or young person) about whom we hold that information would expect us to do so, or have given their permission for us to do so;

(e) hold information securely whether electronic (including the website) or on paper, and hold those records in good order so that they can be retrieved if and when required;

(f) ensure access to the information we hold is limited to those with a strict need to know, and take reasonable steps to ensure the reliability of anyone who has access to personal data;

(g) ensure the information is accurate and up to date;

(h) delete or destroy any personal information as soon as we have no further need for it;

(i) train those who use the information we hold in their duties and responsibilities under the Act.

In particular we ensure that paper records are locked away and that electronic records are password-protected. We also hold back-up copies of our records (both paper and electronic) so that we can recover them in the event of, for example, fire or computer failure.

To reduce the risk of any of the Trustees or employees/volunteers committing an offence under the Act, a central list of all the types of data that we process will be held by the Secretary. The Secretary, who is authorised to act on behalf of Ride High on data protection matters, must therefore be informed of all types of processing of personal data that Ride High undertakes, including any lists or indexes of individuals Ride High receives from other sources.

Individuals (or their parent/carer in the case of children or young people) have a right to know what data we hold about them, whether on paper or electronically. They also have a right to ask us to rectify, erase or destroy inaccurate data. Any requests for details of data held, or for rectification or destruction of such data, should be passed to the Secretary immediately.

Notification to Information Commissioner

The Commissioner maintains a public register of data controllers. Ride High is registered as a data controller. The Data Protection Act requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. To this end the Secretary is responsible for reviewing the Data Protection register annually, prior to notification to the Information Commissioner. Any changes to the register must be notified to the Commissioner within 28 days. Failure to do this is also a criminal offence. Therefore if employees/volunteers are aware of any necessary changes to the register entry for Ride High, they must notify the Secretary immediately.

Disaster recovery

Ride High is also committed to having strategies in place to ensure the recovery of data in any circumstances including fire, hardware or software failure or virus or

hacker attack. Our back up procedures will enable data to be recovered if and when necessary.

Training and awareness

A copy of this Policy will be shown to all employees and volunteers, and each must sign the list attached to the original to indicate they have read and understood it. It will also be made available to all referrers and members and/or their parents/carers.

Any queries that employees or volunteers may have about data protection should be referred to Ann Whitfield.

Approval and review

This Data Protection Policy was approved at a Board Meeting of the Trustees on 17 January 2017. It will be reviewed each September thereafter, or more frequently if appropriate.

Signed.....

Date.....