YoCO
YOUTH CHALLENGE OXFORDSHIRE

Developing young people through personal challenge

Transfer of Information Policy

Introduction

There are occasions when the transfer of YoCO data is required between groups and between third party service providers to perform the functions of the charity. It is essential that any transfer is done in a way that is appropriate for the type of data being transferred. Data can be transferred in a wide variety of media, in electronic and in paper format. YoCO will take the steps set out in this policy to reduce, as far as possible, the risk that exists in every transfer of the information being lost, misappropriated or accidentally released.

When the information is personal or sensitive personal data as defined by the GDPR (see the Data Protection Policy) or considered confidential to the charity it is essential that the transfer is performed in a way that adequately protects the information. Personal information is about a living, identifiable individual. If it contains details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission of offences, court appearances and sentences it is further classified as sensitive personal information. This data is referred to as 'controlled data'.

This policy explains the practical methods that need to be applied when transferring data, especially controlled data. It applies to anyone handling YoCO information who needs to transfer data including:

- Trustees
- Employees
- Volunteers
- Partner organisations
- Third parties

<u>Procedures</u>

1. Before data is transferred it should have the appropriate authorisation from a Trustee and consent of the data owner for the transfer. This especially applies to controlled data.
2. For all transfers of information containing controlled data it is essential that the identity and authorisation of the recipient is established first. It should never be assumed that someone is entitled to the information just because they have said they need it.
3. When dealing with third parties/partner organisations data sharing agreements or contracts in place to cover the transfer of data must be checked. If these have any stipulations in place regarding the method of transfer they must be applied.
4. There should be no more information given than is necessary for the identified purpose. Any unnecessary data must be removed completely before transfer.
5. It is preferable if the purpose can be met by sending anonymised data.
6. The most appropriate transfer of data should be used and consideration of the risks of transferring the data should be made.

Methods of transferring data

Email

1. Controlled data as defined by GDPR should not be sent externally by email as this is not secure.
2. Email messages must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
3. Information sent must, where practical, be enclosed in an attachment.
4. Care should be taken with the information placed in the file name and subject line of the email; these must not show the full contents of the attachments or disclose any sensitive personal data.

Removable storage devices (CD DVD USB and memory stick)

1. When email is not suitable for the transfer of data, removable storage devices can be considered but the devices should be encrypted with a strong password.
2. Clear instructions should be provided for the recipient's responsibilities and instructions on what to do if they are not the intended recipient.
3. An accompanying message or file name must not reveal the contents of the encrypted file.
4. If a removable storage device is lost or stolen this must be reported to the Operations Manager or Trustee as soon as possible.

Internet based collaborative sites (Cloud, Dropbox, Google Docs Office 365)

1. These file sharing programmes are not to be used to share controlled data unless they are encrypted.
2. The Facebook site for each youth group is not to contain controlled data but only information about the events and activities of the group. Each site must be a closed group managed by the group leaders plus the Youth Group Manager.
3. WhatsApp groups are not permitted without the consent of the whole group to share telephone numbers.

Post

1. Letters containing personal information must be accurately addressed and sent to a named recipient as mail going to the wrong person is a danger to the individual whose information is being sent and puts the charity at risk of breaching its GDPR responsibilities.
2. No information relating to another person should be included in the letter.
3. YoCO is responsible for the letter/package up until its successful arrival at its destination.
4. An extra level of protection must be applied if it is necessary to send controlled data eg DBS check information. It must be kept secure, tracked and delivered to the correct individual by using a recorded or special delivery. Successful delivery of the information must be checked as soon as possible. Any issues must be reported to a Trustee immediately.

Transferring Data outside of the UK

1. A Trustee must be consulted before any data is transferred outside the UK. This especially applies to controlled data.
2. Checks must be made that partners or service providers are not planning to process personal data outside the UK eg some service providers may use cloud based systems for data storage which are not UK based.
3. The GDPR requires that personal data must not be transferred to a country or territory outside the UK unless that country, territory or third party can provide an adequate level of protection for the rights and freedoms of the individuals whose data is being transferred.

4. Volunteer forms used by the Nasio Trust are never transferred abroad and an encrypted Dropbox is used for essential medical information. The volunteer medical information form has the following:
   'Medical information will not be shared with any other party unless necessary for the safety of the volunteer, other group members or Nasio staff. In this event; strictly relevant information only will be shared with the Nasio team leader. If you have any concerns about any especially sensitive data, please discuss with the Nasio UK office so that we can ensure full confidentiality whilst protecting the volunteer and others.'

Reporting Data incidents

All trustees, staff and volunteers must report any suspected or actual security breaches related to the data to the Chair of Trustees immediately.

This policy was adopted at the Board of Trustee Meeting on 19st January 2022

On behalf of the Board of Trustees Jane Cranston…….. (signed)

This policy will be reviewed annually by the Board of Trustees; Review Date January 2023