fota
Friends of the Award
EDINBURGH AND THE LOTHIANS

DATA PROTECTION POLICY

Introduction:

FOTA is a charity which supports the delivery of the Duke of Edinburgh's Award (DofE), Junior Award Scheme for Schools and other accredited learning programmes in Edinburgh and the Lothians.

FOTA is committed to ensuring that data is effectively managed and properly protected.

In preparing this document FOTA is aware of the requirements of the forthcoming General Data Protection Regulation (GDPR).

Data:

Much of our work involves direct delivery of the DofE to young people on behalf of our local authority partners. Data associated with this work is owned by said partners and our staff work directly to their policies and protocols. In addition, our work with young people with mental health issues is in partnership with NHS Lothian Children and Adolescent Mental Health Service. Data sharing on this project conforms to their policies and protocols.

FOTA holds the following Data:

Personal information relating to the young people we are working with in our projects including their contact details, photographs, and records of progress through their DofE or JASS programme.

HR records and contact details in relation to our staff team and volunteers.

Business management information in relation to our accounting, budgeting, fund raising and project management.

Business information, including customer and distributor details in relation to our promotion and delivery of JASS.

Corporate information in relation to the management and governance of our charity.

Promotion and evaluation materials.

Security of Data:

FOTA is committed to ensuring that we only retain Data legally obtained, that it is not held for longer than required for the purpose and is held securely.

Hard Copy Data:

Hard copy data will be retained in our office at The Risk Factory, 20 New Mart Road, Edinburgh. The office will be locked, when unoccupied and the building is secured by an alarm system managed by City of Edinburgh Council.

On occasions when hard copy data is removed from the office by staff or volunteers, they will take all reasonable steps to ensure that it remains secure.

Hard copy data will be disposed of by shredding or burning.

(See also ***Appendix A re retention of photographs***)

Electronic Data:

All electronic data is retained on FOTA computers which are protected by Norton 360 Security.

FOTA computers are password protected.

FOTA uses Google for email, contact database and calendars. This system us password protected.

All our operational Data is retained on Microsoft One Drive which is password protected. (From Spring 2018)

FOTA data must only be downloaded to FOTA computers. Staff and volunteers accessing FOTA data from remote locations must only access and save to our One Drive cloud.

E'JASS data is fully covered by a separate policy – ***see Appendix B***

Password Policy:

Passwords must be a minimum of eight characters and use a complex character set that has a mix of upper and lower-case letters at least one of which is non-alphabetic.

Be changed a minimum of every 12 weeks.

Passwords must not be re-used within 20 password changes.

Retention of Data:

Data will be retained only while it is required for the purpose for which it has been gathered or to meet the legal requirements on our charity.

Personal Data:

Data relating to ***job interviews*** in respect of unsuccessful candidates will be retained for 6months.

All data relating *to* ***employees***, including interview papers, will be stored electronically on our One Drive with access restricted to Project Manager and Chair. They will be destroyed 6 months after the employee has left the charity.

Data in relation to our ***volunteers*** will be retained for the same period as that pertaining to employees.

Experience has shown that adults (Staff and volunteers) who attend our courses sometimes request details of their courses and qualification for several years after the course. For this reason, data in relation to our ***training courses*** will be retained for 5 years following the course.

Young people attending any activities, including expeditions, in relation to our accredited learning programmes routinely 'opt out' for a number of years, then return to complete their DofE or other programme at which time they require

information to complete their records. We will retain this data for a maximum of 6 years.
Photographs will be retained for a maximum of 4 years. The exception being our Annual Reports which contain photographs, and which will be retained indefinitely.
E'JASS records will be retained for six years. This allows for participants to work through the four years of their JASS programme and for records to be available for 2 years beyond this time.

Other Data:

Financial Data, Minutes of Meetings and other data required by HMRC, Companies House or OSCR will be retained in line with their requirements.
All other data, including grant applications, reports to funders, evaluation reports and training materials will be retained as long as it is relevant to the efficient management of our charity and delivery of our work.

Individual's Rights:

FOTA fully respects the rights of individuals in relation to their data which we hold. We will be fully transparent with regard to what information we retain, the purpose of holding the information and our weeding policy in relation to personal data.

Where an individual requests that we delete their personal data, unless there legal reasons requiring our retention of that data, we will take all reasonable steps to have that data deleted from our electronic systems or shredded if in hard copy.

Subject Access Requests:

FOTA will consider all subject access requests and provide the information requested to anyone entitled to it within 14 days.

Data Protection by Design and Data Protection Impact Assessments:

General Data: FOTA has fully considered the storage of electronic data required to deliver the work of our charity. Consequently, we have entrusted our data to cloud storage provided by Microsoft One Drive (from Spring 2018) which is a respected provider of secure data storage. Similarly, we have opted to use Google as our provider for email and calendar function.
E'JASS: The processes for retaining the security of data on our E'JASS platform is outlined in Appendix B. In considering the ongoing security of personal data in relation to E'JASS participants we intend to move to a fully randomised participant numbering system during the summer 2018. This means that the only personal data held on each participant on the system will be their name. With over 12,000 participants worldwide, it will be almost impossible for anyone illegally accessing the system to identify any individual participant.
Training: A training powerpoint presentation will be used to brief all staff members on the relevant aspects of our Data Protection Policy and this will be followed by a questionnaire to test their understanding.

Data Protection Officers:

A member of our Board will have overall responsibility for data protection compliance and access. Our Project Manager will have day to day responsibility for the implementation and compliance.

Review:

This policy should be reviewed in 12 months to ensure that it is compliant with new legislation. (April 2019)

Appendix A: Retention of Photographs:

1. **Consent to Use Photos**
For outdoor and indoor activities we will use the City of Edinburgh Council EE2 consent form as permission to use photos.

2. **Archival of Consent**
The original EE2s will be archived in folders per activity and stored in an archive box in the stationery cupboard. As per City of Edinburgh Council Policy these will be kept there for at least 3 full years after the event but no more than 4 years. A scanned copy of the relevant consents will be archived along with the photos as per action point 4 below.

3. **Collection of Photos**
FOTA staff, volunteers and partners may supply photos which may be used for marketing/reporting purposes. If photos are supplied by partners you will **not** require full individual consent but we will require a statement from the partner to say that they have consent from participants to take photos and that they allow us to use these for marketing/reporting purposes. Once supplied to FOTA, staff members and volunteers should **not** keep copies of any photos containing young people's faces.

4. **Archival of Photos**
FOTA will keep 3 full years of photos and all photos plus a scanned copy of all EE2 consent forms be archived on a portable hard disk and stored in the stationery cupboard. Photos and accompanying scans of consent forms will be archived together in folders by year, subfolders by project and further subfolder by event. No specific record of participant's names should be kept as this creates additional data collection.
Photos supplied by partners should be stored along with the partner's consent form.

   A second copy of photos will be stored in a shared folder in the One Drive but this should **not** include consent forms.

   After 3 years (but no more than 4 years), photos and consent form should be deleted from both the archive and One Drive folder.

5. **Use of Photos**
Photos can be used for any FOTA and CEC funding/marketing purposes but the photos should **never** be more than 3 years old. Older marketing materials may be distributed even when the original copy of the photo (and consent) have been destroyed but newly created materials should not include photos older than 3 years.

6. **Longer Use of Photos**
   Longer term usage of particular photos can be agreed with an additional consent form. The additional consent form should contain Name, Date of Birth, Address of Participant and a statement that FOTA have permanent ability to use the photos. The additional consent must be requested within one year of the activity.

7. **Removal of Photo**
   Should a person request that a particular photo not be used, we must follow their request and remove the photo from accessible locations e.g. website, One Drive and archive folders. We would not be able to recall or redesign print or published materials so we should retain their consent form should we later be asked to prove consent for using the photo in these materials.

   Should a person request that we stop using photos of them, we may need to ask them to supply a photo or come into the office so that we can identify which photos include their face. We would then follow the same procedure.

Appendix B Privacy and Security Policy for E-JASS

Data Storage

The E-JASS system has been designed as an online tool to support the JASS award scheme. The data stored by the system corresponds with that needed to complete the award.

Data used by the system for schools and individual participants is:

Data Stored	Description/Notes
A unique username for each participant.	For participants this is usually their Scottish Candidate Number. For mentors this is usually an email address.
Names	The first name and surname of all users is stored within the system.
School Name	The name of the school associated with each user.
Local Authority Association	For some schools who are part of a bigger organisation such as a local authority, this information is related to the school within the system.
Class or Group Name	A class or group name is stored for each mentor. This name may or may not represent an actual physical group that exists within the school.
Activity information	Participants are required to log their activities as part of the award scheme. Activity information includes: ● The name of the activity ● A description of the activity ● The time taken to complete the activity ● Personal reflections on the activity ● Evidence of the activity. (Evidence of the activity can includes images, documents or video.)

Mentoring information	Mentors can provide feedback to participants in the form of a text comment. This information is stored within the participants activity information.
Award Progress	The amount of accumulative time and the status of an award (not completed/completed) is stored for each participant.

Data Sharing

No information or data is shared with any third-party organisations. Data can only be accessed by authorised persons within the school and within JASS.

Data Analytics

No third-party tracking or analytics services (such as Google Analytics) are used.

JASS administrators are provided with a high level overview of customer accounts and participant progress. These include

- The number of participant accounts currently set up within an organisation
- The number of active participants completing awards
- The number of awards completed

These reports do not include any identifying information about participants, nor do they include access to participant activity details.

Access to Data by JASS Staff

All JASS staff are members of the Disclosure Scotland PVG scheme.

The E-JASS system provides a layered user access policy to limit the visibility of individual participant activity to that of their mentor. School administrators and JASS administrators have no direct access to participant activity.

A privacy impact assessment (P.I.A.) has been carried out as per Information Commissioner guidelines

Data Retention

Participant data is kept for a duration long enough that the user is able to complete the bronze, silver and gold awards of JASS, providing that the participant is associated with an active customer account.

In the event that a school does not maintain an active JASS account, all user data is made inactive within 30 days of cancellation. After an additional 30 days, all data with those accounts is permanently deleted there is no possibility of data reinstatement should the account be reactivated.

Data Security and Policies

JASS is working with City of Edinburgh Council to ensure that our data security policies and procedures meet the required standards and work towards ISO27001 and the UK Cyber Essentials requirements.

Overview of the E-JASS Application

E-JASS is a web application which is accessible by users via any standard Internet connected web browser. Currently, there are no mobile apps available.

Hosting

Hosting is provided by Linode (www.linode.com) and all servers are located in Linode's London data centre. Linode provides a high level of security (including physical security) to the servers within the data centre.

Data storage devices are shredded when decommissioned.

Linode's network infrastructure provides an number of software security features outside of those applied at the E-JASS application server level. These include additional firewalls and DDoS prevention.

The E-JASS Web Application

Infrastructure and Application Specific

- Multiple app and databases servers are used and all are hosted with Linode's data centre
- All servers are virtualized and the integrity of the systems and data is maintained by Linode's systems
- Systems are monitored for potential hardware failure and performance - either due to suspicious activity or increased user generated load
- Cookies are used only to maintain active session logins
- Data is backed-up daily. Backups are maintained for up to 30 days.
- The web application requires a standard web browser. No plugins (e.g. Flash and Java) are needed).

Security

- Servers are protected by individual firewalls, IDS and antivirus software.
- User access is authenticated using username and password
- Administrator access to the server is restricted by IP address
- All user access including file uploading is provided over HTTPS
- OS and application software patches are applied on a monthly basis
- Access logs are kept for 6 months.
- File uploads are restricted to prevent certain dangerous file types from being uploaded (e.g exe files)
- The web application is built using industry standard tools and frameworks which are regularly maintained
- A penetration test in conducted every 6 months
- The application adheres to OWASP principles