Data Protection, Confidentiality and Security of Information Policy & Procedure

Date: 15th November 2018

Table of Contents

Key Terms

General Data Protection Regulation (GDPR) - regulation in EU law on data protection and privacy for all members of the European Union. It aims to give individuals control over their personal data.

Data Protection Act 2018 - Act intended to apply the EU GDPR standards to English Law.

Data Controller - an organisation that determines the purposes and means of processing personal data. The GDPR applies to data controllers such as KEEN.

Personal Data - any data relating to an identifiable, living individual. This includes name, address, personal attributes, characteristics, habits, preferences and choices. This also includes one's unique identification such as NHS number, National Insurance number and potentially a database ID number, and IP address of our personal computer.

Sensitive information - a specific sub-category of personal information with designated special categories of data that must be treated with special care. Under the GDPR, these categories are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data; and
- Biometric data (where processed to uniquely identify someone).

Financial information - a person's payment details; held by KEEN if they need to pay subscriptions or if the person pays for their own service.

Information Security - the protection of information and information systems from unauthorised access, use disclosure, disruption, modification or destruction.

Data protection principles - The GDPR sets out 7 key data protection principles:

- Personal data must be processed in a lawful, fair and transparent manner.
- Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data processing must be adequate, relevant and limited to what is necessary in relation to what is necessary in relation to the purposes for which they are processed.
- Data must be accurate and up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without

delay.
- Data must be kept in a form which permits identification of the individual for no longer than is necessary for the purposes for which the personal data is processed.
- The data must be processed in a manner that ensures appropriate security of the personal data.
- The Data controller is accountable for their compliance with these principles.

Personal Data Breach - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Introduction

The GDPR and the Data Protection Act 2018

From 25th May 2018, data protection law has been determined by the GDPR (General Data Protection Regulation) and the Data Protection Act 2018. These replace the Data Protection Act 1998 and The Privacy and Electronic Communications (EC Directive) Regulations 2003.

This policy aims to be as compliant as possible with the GDPR and the Data Protection Act.

What does it apply to?

Data protection principles must be introduced into the charity's personnel (in terms of culture and training), processes (how we do our business each day) and technology (how we use electronic and mobile technology to store and use data).

Data protection rules relate to personal data. Sensitive personal data requires additional rules and safeguards.

The need for this policy

In undertaking our various activities KEEN finds it necessary to hold various items of personal information. This Data Protection, Confidentiality and Security of Information Policy & Procedure document describes how this information will be kept and managed with the intention of complying with the Data Protection Act 2018 and ensuring that information is retained for the minimum period of time and in a safe and secure way.

Our Data Protection and Retention Policy has been developed specifically to meet the requirements of the Data Protection Act 2018 and to represent good administrative practice.

It is our understanding that KEEN does not need to register (and is therefore not registered) with the Information Commissioner's Office as we qualify for the following 'not-for-profit' exemption:

"You must:

- only process information necessary to establish or maintain membership or support;
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- you only hold information about individuals whose data you need to process for this exempt purpose;
- the personal data you process is restricted to personal information that is necessary for this exempt purpose;
- only keep the information while the individual is a member or supporter or as

long as necessary for member/supporter administration”

Keen as a Data Controller

Under the law, KEEN is a data controller for all personal data we hold regarding our employees, volunteers, athletes, members, families of athletes and members, and also many of our supporters and donors. KEEN is exempt from registration with the Information Commissioner’s Office as a data controller. However, it tries to ensure that all personal data is dealt with in accordance with the data protection principles in any event.

All staff are required to be familiar with the meaning of personal data, sensitive personal data and the data protection principles and to comply with those principles to the extent appropriate to their level of responsibility. In this context, all staff are also required to comply with the procedures referred to below on Confidentiality and Security of Information.

Our objectives

- For KEEN to collect and retain the minimum information needed to function as a charity and to operate against our other policies and operating requirements.
- When collecting data or information of any kind we will at all times be clear about specifically what information we are asking for, why we are asking for it and what we will do with it once we have it.
- At all times KEEN will apply the highest levels of data protection that are practical, possible and affordable.
- We will review and refresh the information that we hold on a regular basis and will set time limits for data retention.
- Once we have finished with the information we hold we undertake to dispose of it in a responsible manner that will not compromise the privacy of anyone.

Scope of the policy

This policy applies to all employees, volunteers, athletes, members, families of athletes and members, and also many of our supporters and donors who handle KEEN information.
This policy relates to all personal information controlled by KEEN whether merely held or created by the organisation.
This policy covers all information management, processing and information storage activities partaken in by KEEN whether stored electronically or as physical copies.

Responsibility for the policy

The Executive Director is the organisation’s Data Protection Officer and is responsible for ensuring that all staff and volunteers are aware of their responsibilities under data protection law and for ensuring that KEEN complies with current data protection law (whether or not the current law is properly reflected in this policy).

In cases of uncertainty in any given situation, advice must be sought. Staff are asked to refer any queries to the Data Protection Officer, who has day to day responsibility for ensuring KEEN’s compliance with the legislation.

Purpose of this document

This document is an addendum to KEEN's Policies, Guidance Notes and Procedures document and is intended to be used alongside the existing policy.

Receiving, Retention and Disposal of Data

KEEN keeps data in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods in so far as the personal data will be processed solely for scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by law in order to safeguard the rights and freedoms of individuals.

Receiving Data

All requests for data will be reviewed by at least 2 trustees who must confirm that they are content that the request is clear about specifically what information we are asking for, why we are asking for it and what we will do with it once we have it.

Retention of Data

It is KEEN's policy that the data we retain will only be held subject to the following standards:

Accurate and up to date
KEEN aims to hold accurate and up to date information and we take every reasonable step to ensure that personal data is reviewed and updated, as necessary.

Secure retention of data
HR files are kept securely in locked cabinets with access to them managed on a day-to-day basis by the KEEN Coordinator. The cabinets are themselves stored in locked offices during non-working hours.

Right to give and withdraw consent
Data will only be held so far as is consented to by our employees, volunteers, athletes, members, families of athletes and members, supporters and donors. If this consent is not given or is later withdrawn, the data will be disposed in the usual way.

Specified, explicit and legitimate purpose
All data collected for specified, explicit and legitimate purposes will not be further processed in a manner that is incompatible with those purposes. Any use for scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes.

Storing what is necessary
KEEN will hold personal data that is adequate, relevant and necessary for the purposes for which it is being processed. This purpose will be recorded at the time that the data is requested or received. **Any individual can ask at any time for what purpose we intend to use their information.**

The necessary periods of retention and purposes for the retention of data from respective members of the KEEN community are listed below:

Job Applicants
Personal information received during the recruitment process will be retained until selection is made and the person selected has signed the contract for the role concerned.
If an unsuccessful applicant would be suitable for another position that may become available in the future, we will ask for permission to retain personal information to retain information for the appropriate period agreed with the applicant at the relevant time.

The application pack of the successful applicant/employee will be retained as part of their Human Resources (HR) file which subsequently will contain staff assessment information and any other HR information which is necessary for the efficient operation of our management and supervision processes.

Employees
Once a person leaves our employment, we retain their information on our accounting system for a minimum of 4 years after their departure for audit purposes and in order to process any queries relating to their pensions or other payments.

The person's hard copy and/or electronic HR file is also retained for 4 years, after which time it will be deleted or destroyed. We have an electronic record of the dates when a person's HR information should be destroyed. This is checked twice per year during an internal audit process.

Staff may ask to see their HR file at any time. Consent to hold this information is given when they sign their employment contract.

Volunteers
Volunteer information comprises of the data given to us at the recruitment stage with addition to information such as training courses completed, DBS checks approved and performance data. We will destroy volunteer information within 5 years of a volunteer formally leaving us. We retain information for this period in case they decide to return or in case a query arises about a particular incident at a service. It also enables us to find the volunteer's role and performance details in the event that they ask us for a job reference.

Participants and their families
Children, young people or adults using our services and their parents or carers (our clients) provide personal details prior to attending a service. Normally this is via a paper or an electronic form although it could be provided verbally.

All Athlete and Member Profile cards should be reviewed and updated annually. If an Athlete does not attend any KEEN session for two years, their Profile card must be destroyed.

The information should enable staff to communicate with the person and their family, handle emergencies, arrange transport, report on aspects of KEEN's performance to funders (including sensitive personal information such as type of disability and ethnicity), and implement safe care whilst the person is with us. This may include personal care, medication, moving and handling information, and equipment needs.
We also hold financial data if a person needs to pay subscriptions or if the person pays for their own service via a person budget. The purpose of all data we hold is either to deliver the best possible services to clients or to report effectively to funders on how well we are meeting their required performance targets.

Supporters and Funders
We may hold the contact details for funders, potential funders and supporters, some of whom may be individuals (such as major donors). We obtain this information from the individual concerned ensuring that they provide us with written authority for us to contact them for the purpose of fundraising.

We may hold the bank details of our current funders or other sensitive personal information, if necessary for funding purposes. **We will delete or destroy all data with 5 working days of the person requesting this.** We will routinely remove all such information from our systems and hard copy files as soon as it is clear that KEEN no longer will need to use it for the purpose for which it was originally provided.

Whilst we do not ask for a person's data directly for fundraising reasons, we reserve the right to communicate with our supporters in a reasonable, polite and responsible way about such matters e.g. sending out membership requests, newsletters, information that they may find interesting (such as the KEEN Annual Report) and information about the charity's work which could help people to raise funds on our behalf.

Return of all documentary information

All documentary information, whether in hard or soft copy form, given to or acquired or created by any staff member or volunteer in the course of and relating to their working with KEEN must be returned to KEEN at the end of the working relationship.

Requests under the right of subject access

Any person for whom we hold or may hold personal data can request that they see a copy of the information stored. We will comply with any such request within 30 days.

If the person asks us to correct or update the data we hold, we aim to do this within 5 days of the request.

Any staff member receiving any request which is or may be a request under the *right of subject* access must immediately refer the request to the Executive Director.

All requests to access this information must be considered by the Data Protection Officer and the Data protection Officer must manage the process of access to ensure that all records are replaced and that no unauthorised (and therefore uncontrolled) copies are taken. Any copies of information that are required for a legitimate reason must be managed as rigorously as the originals.

Disposal of data

All paper records will be disposed of by shredding in such a way as to render the information illegible. All electronic records should be destroyed using appropriate software.

Security of Information

It is KEEN's policy to have in place operational measures to ensure that information relating to its business and activities is kept secure and in a manner consistent with current law, regulatory requirements and recommended practice.

Scope

This policy applies to all members of staff who may handle KEEN information. This policy relates to all information stored or processed by KEEN both in hard copy and electronic form.

Governance

The Executive Director has day to day responsibility for security measures. All staff members are responsible for ensuring that all personal information, financial information and sensitive information with which they may come into contact in their work with KEEN is kept secure by them in accordance with the law and with these policies and procedures, and are required to report any matters of concern relating to the security of such information to the Executive Director as soon as possible.

Procedure

Information in hard copy form

Personal information, financial information and sensitive information in hard copy form, wherever held, is required, when not actively being used, to be kept in locked drawers/filing cabinets/cupboards, with access to relevant keys and knowledge of their location being restricted to staff who may need access to such information to carry out their duties.

When in use, this information should be out of sight, and if possible, be in a locked or secured place where there is minimal chance of clients, client's families or others (the general public or security staff) being exposed to it, whether accidentally or on purpose.

All such information when being taken from one place to another is required to be kept under the direct control of the person responsible for it in as secure a manner as is practicable in all the circumstances. This would normally mean a zipped bag or container with KEEN's contact details clearly marked, so that it can be returned easily in case of accidental loss.

No such information should be posted unless authorised by the relevant projects manager, the Executive Director or Chair of Trustees for the efficient running of KEEN's business and activities. Original documents of which no copy exists should, wherever reasonably possible, be copied before posting.

Information held electronically

KEEN may choose to hold personal data in an IT system stored off-site, for example with a cloud provider. We will ensure that there are reasonable measures in place to ensure full security of personal data and these terms will be made available to individuals upon request. If implemented correctly, off-premises data storage can offer the same or better security than on-premises solutions. We will take all necessary steps to ensure that this is the case and will make security of personal data the highest priority when deciding on any IT system or process.

Personal information, financial information and sensitive information in electronic form must be subject to password access for individual authorised users only, authorisation being restricted to staff who may need access to such information to carry out their duties.

All such information when being taken from place to place, in particular on any portable equipment or media (such as laptops, tablet computers, memory sticks and memory cards), is required to be kept under the direct control of the person responsible for it in as secure a manner as is practicable in all the circumstances. All smart phones, laptops and tablets must have a secure password or code that is necessary to turn on and use the device, in addition to the passwords needed prior to using any online IT system and the passwords attached to the files or data storage system themselves.

Any electronic data or information must be located and/or accessed via a computer which has high levels of encryption, protected by a firewall provided by a reputable vendor and protected by an up-to-date and effective anti-virus programme.

Passwords must not be changed by staff without informing the Executive Director at the same time. The Executive Director must have a record of all passwords used for all KEEN devices that contain this kind of information.
Any computer used to access KEEN information must be password protected to a high level. The password must be at least 6 characters in length, at least 5 different characters, 3 classes of characters (classes are uppercase letters, lowercase letters, digits and punctuation characters). It must be renewed at least every 8 weeks. No KEEN computer containing information must be left on and 'logged-in'. The operator must press 'ctrl+alt+del' and select 'lock this computer' before leaving it.

Breach

All staff have an obligation to report actual and potential data protection compliance failures to the Executive Director who shall investigate the breach. Breaches must be reported to the individuals affected and the Chair of Trustees. The executive director will report it to the ICO when necessary. This will take place within 72 hours of a personal data breach being found

and where there is likely to be a risk to people's rights and freedoms as a result of the breach. A log of data protection compliance failures will be kept.

When reporting such a breach, the GDPR requires that the following information is provided:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Confidentiality

It is the policy of KEEN to keep confidential all personal information, financial information and sensitive information. It is important that we maintain the confidentiality of our Athletes, Members and Volunteer coaches, especially when referring to incidents that involve them.

Confidentiality Procedures

All written material containing detailed information about Athletes, Members and Volunteer coaches should be marked 'Confidential' and access restricted as appropriate but not in a way to prevent it being used for the purpose for which it was created.

Any publicly available documents should refer to the person's initials. Where specific communication is required for instance by email, then the title of the email should be 'Confidential' and the recipient should then treat the contents of the email in the appropriate manner.

Personal Information

Personal information, whether in hard or soft copy form, for example, names and contact details of athletes and members and details of their needs, should only be accessed by staff and volunteers to the extent necessary for the performance of their duties in connection with their activities for KEEN.

Personal information, whether in hard or soft copy form, should not be held by any staff member outside KEEN's offices, save to the extent necessary for the carrying out of KEEN's activities in a lawful, proper and efficient manner. Personal information so held is the responsibility of the individual holding it.

Personal information, whether in hard or soft copy form and wherever held, should not be left unattended or visible in a public place when in use and must be stored securely when not in use. For example, care plans for use at a project session will need to be accessible to all staff and volunteers, if needed, but should be kept out of sight and not within easy reach of clients or their families.

They should be stored in a place and manner such that they cannot be accidentally moved or mistakenly taken by others. If possible, there should be a secure cupboard or drawer at each setting for this purpose which can be locked or otherwise safely protected.

Any loss of personal information or suspected loss of information, in whatever form, must be reported as soon as practicable to the Executive Director, or, in his absence, the Chair of Trustees.

Personal information, in whatever form, must not be disclosed to anyone outside KEEN save as referred to below.

Financial information

Financial information, whether in hard or soft copy form, should only be accessed by staff to the extent necessary for the performance of their duties in working with KEEN.

Financial information, whether in hard or soft copy form, should not be held by any staff member outside KEEN's offices, save to the extent necessary for the carrying out of KEEN's activities in a lawful, proper and efficient manner. Financial information so held is the responsibility of the individual holding it.
Financial information, whether in hard or soft copy form and wherever held, should not be left unattended when in use and must be stored securely when not in use.

Any loss of financial information, in whatever form, must be reported as soon as possible to the Executive Director, or, in his absence, the Chair of Trustees.
Financial information, in whatever form, must not be disclosed to anyone outside KEEN save as referred to below.

Sensitive information

Sensitive information, whether in hard or soft copy form, should only be accessed by staff or volunteers to the extent necessary for the performance of their duties in working with KEEN.

Sensitive information, whether in hard or soft copy form, should not be held by any staff member outside KEEN's offices, save to the extent necessary for the carrying out of KEEN's activities in a lawful, proper and efficient manner. Sensitive information so held is the responsibility of the individual holding it.

Sensitive information, whether in hard or soft copy form and wherever held, should not be left unattended or visible in a public place when in use and must be stored securely when not in use. For example, care plans for use at a project session will need to be accessible to all staff or the relevant volunteers, if needed, but should be kept out of sight and not within easy reach of clients or their families.

Sensitive information should be stored in a place and manner such that this cannot be accidentally moved or mistakenly taken by others, such as office security staff. If possible, there should be a secure cupboard or drawer at each setting which can be locked or otherwise safely protected.
Any loss of sensitive information, in whatever form, must be reported as soon as practicable to the Executive Director or, in his absence, the Chair of Trustees.

Sensitive information, in whatever form, must not be disclosed to anyone outside KEEN

unless we are obliged to by law or with specific permission from the person in question or guardian.

Retention and disposal of personal, financial and sensitive information

Personal information, financial information and sensitive information, in whatever form, will be held for such period, depending on its nature, as complies with recommended practice on retention of information. In particular, information relating to any safeguarding issue will be kept indefinitely and financial information will be kept for a minimum of 7 years.

Personal information, financial information and sensitive information in hard copy form will be shredded or disposed of in confidential waste bins. Personal information, financial information and sensitive information held electronically will be deleted from the relevant equipment and media.
Equipment and media which has contained personal information, financial information or sensitive information will be disposed of in such manner as ensures that any residual information is securely deleted during the disposal process.

Disclosure of information outside KEEN

Disclosure Policy

Personal information **must not** be disclosed outside KEEN unless those to whom it relates gives their consent for its use for the specific purpose concerned, or unless its disclosure is required by law or other regulatory requirements.

Financial information **must not** be disclosed outside KEEN, without the consent of the Executive Director and the Chair of Trustees or as required by law or other regulatory requirements.

Sensitive information *must not* be disclosed outside KEEN unless those to whom it relates give their consent for the specific purpose concerned or its disclosure is required by law or other regulatory requirements.

Further guidance on personal and sensitive information is available in:

- KEEN's Safeguarding and Protecting Children and Vulnerable Adults Policy

Avoiding casual disclosure of information

All staff are required to take all reasonable measures to ensure that:

- when using any personal information, financial information or sensitive information, in whatever form and in whatever circumstances, such information is not seen by any person who is not authorised to see it, and
- when discussing any personal information, financial information or sensitive information, in whatever circumstances, such information is not heard by any person who is not authorised to hear it.

Exemptions to disclose

In the context of safeguarding children and safeguarding vulnerable adults from abuse, sensitive information may need to be shared as provided for in:

- KEEN's Safeguarding and Protecting Children and Vulnerable Adults Policy

Staff should refer to the relevant policy and procedure if they feel sensitive information needs

to be shared in any given case. Volunteers should not share information under any circumstances but must refer the case to the Executive Director. In any event, save in cases of emergency, staff must refer to the Executive Director, as the nominated safeguarding children adviser or the responsible person for safeguarding vulnerable adults, for guidance.

Third-party use of data

KEEN will never sell personal information to a third party or provide it to a third party for any purpose unless we are legally obliged to for safeguarding purposes or as part of a criminal investigation or with specific permission from the person in question themselves.

We may provide anonymous or summarised data to organisations for academic research purposes. We do not intend to buy donor information from a third party.

Data will 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.

Equipment or media containing any personal information, financial information and sensitive information will not be posted under any circumstances.

Specific Arrangements

The precise arrangements showing, in detail, how KEEN manages the provisions set out in this policy are set out in a separate, operational document, titled 'KEEN– arrangements to ensure data protection'. Due its nature, that document does not form part of this policy and is only available to KEEN management.

Staff and Volunteer Training

All new staff and volunteers sign a confidentiality statement prior to starting work for KEEN. A key element of the staff code of conduct and our volunteer agreements is the requirement for staff and volunteers to follow the law relating to data protection as well as KEEN's own policy and procedures relating to confidentiality and the handling of personal data.
Failure to do so may result in disciplinary action. A serious breach of security, e.g. putting an athlete's personal data at risk, would be cause for summary dismissal at the discretion of the Executive Director.

Volunteers will receive data protection and confidentiality training and will receive regular briefings with regard to security procedures both in the office and off site.

This will be updated periodically. Staff and volunteers must ensure that they are particularly vigilant if they have responsibility for updating, storing or transporting personal information e.g. holding care plans at project sessions.

Internal Audit Guidance

Check	**Evidence**
Staff know which Act underpins the rules for managing data	Ask staff (either 1:1 or in group setting)
Staff are aware what personal data and sensitive personal data is	Ask staff (seek examples)
Staff know what their responsibilities are in relation to the following provisions within this document:	Ask staff Observations in the office

Review

This policy shall be reviewed annually. It was last updated in November 2018. The next review will take place on or before November 2019.