Data Processing Policy

1. Introduction

The Staff College: Leadership in Healthcare (SC) has a data protection policy in place which outlines the broad general data protection regulations and principles with which it must comply. It has developed a 'Data Processing Policy' in order to identify the data that the charity holds, why it holds this data, how long it is kept for and explain how it is processed. This policy will be made readily available to Staff College members and the general public so that they are able to understand and have confidence in the way that their personal data is processed, if applicable.

In order for the charity to operate effectively, it needs to process and store several types of data from a variety of different sources. The charity has an overview of the data that is currently holds at any one time and retains a copy of the consents for keeping this data.

Contents

2. Types of data the charity holds, how it seeks and records consent

2.1 Contact details for distribution lists of newsletters and charity updates

In order to work effectively as a charity, we need to ensure we can stay in contact with our members, commissioners and supporters.

What data we hold	• Name • Email address
Why we hold it	• So, we are able to contact our members, commissioners and supporters. • So, we can provide regular updates of the work the charity is involved in. • So, we can provide details of upcoming courses and application deadlines. • So, we can send out invitations to our lectures and events. • So, we can ask for input on particular issues from our members.
How we hold it	• Database of contact details stored on mailchimp.
How do we seek consent to hold it	• All contacts will be asked to sign up manually via mailchimp and consent to be on our mailing list by 1 Mar 2018. • All those currently on our mailing list will be contacted 31 Oct 17 to be asked to sign-up manually. • All those who don't sign up manually will be deleted from our distribution list on 1 Mar 2018.
How we record consent	• Consent records automatically compiled by Mailchimp
How long we hold it for	Ongoing
Process for deletion of records	Should a member decide they no longer wish to receive updates they can unsubscribe either by contacting the SC team, or by selecting unsubscribe from one of the emails.

2.2 Members training records

What data we hold	• Name • Job title • Organisation • Email address • Phone number • Details of who is supporting application: name, job title, organisation, email address, phone number • Details of who is funding the applicants' course fees: name, job title, organisation, email address, phone number • Goals for attending the course • Date of course attendance
Why we hold it	• So, we know who is attending the course and how to contact them to provide necessary course information. • So, we can advise members on appropriate follow up courses. • So, we know who is supporting the applicant in case there are any issues that need to be raised around non-attendance. • So, we know who is funding the course fees so we can invoice and follow up for payment for these. • So, we can report on numbers and backgrounds of those we train.
How we hold it	• Records are input onto a protected members database. • Copy of members application form is stored electronically.
How do we seek consent to hold it	Application form with signed consent to hold training records and take part in the course activities.
How we record consent	Electronic copies of application forms are saved on charity's shared drive.
Process for deletion of records	At the beginning of each month, all training records relating to attendance on courses 12 months previously are deleted from database and application form is deleted.

2.3 Training records of members who attend programmes commissioned by other organisations: i.e. who don't apply directly to SC to attend a course.

Where SC is asked to deliver a programme on behalf of another organisation, the commissioning organisation is the data controller. SC and the data controller will agree at the outset, whether SC will maintain a training record for those who attend a programme:

1. If the data controller prefers SC not to retain a training record, then SC will not retain a training record, and will instead maintain an anonymised set of statistics regarding the number of members trained, and a breakdown of the specialties that they come from.

2. If SC is to maintain a training record for those who attend a programme, the data controller will seek explicit consent from all attending that they can share this data with SC as a third party. The data will be stored in the below way.

3. Where there is any concern whether explicit consent has been sought for SC to hold data during the contracting phase, SC will ask all participants to complete a consent form which outlines how their data will be held prior to them holding this data.

What data we hold	• Name • Job title • Organisation • Email address • Phone number • Date of course attendance • Any supporting details provided on their application forms which bear a relevance on the programme. E.g a project a member is working on in relation to the programme.
Why we hold it	• So, we know who is attending the course and how to contact them to provide necessary course information. • So, we can advise members on appropriate follow up courses. • So, we can report on numbers and backgrounds of those we train.
How we hold it	• Records are input onto a protected members database. • Copy of members application form is stored electronically.
How do we seek consent to hold it	Data controller provides application form and seeks signed consent to hold training records and take part in the course activities.
How do we record consent	If applicable, electronic copy of consent forms are stored on SC's shared drive.
How long we hold it for	From point that application form is submitted to the beginning of the month after the first anniversary of the date of attendance on course.
Process for deletion of records	At the beginning of each month, all training records relating to attendance on courses 12 months previously are deleted from database and application form or consent form is deleted.

2.4 Anonymised forms for the monitoring of equality and diversity

SC is committed to monitoring whether the courses it delivers reach and audience reflective of the workforce of the health service. For its internal programmes, it actively asks members to complete a voluntary equality and diversity monitoring form at the end of courses and reports on the findings in these.

What data we hold	Anonymised equality and diversity monitoring forms.
Why we hold it	So, we can monitor the levels of those attending our courses from different backgrounds and with different characteristics, in order that we can identify whether we are reaching a fair and diverse audience. If we're not, then we can develop a plan to reach out to those from different backgrounds who aren't being fairly represented.
How we hold it	Anonymised forms are stored electronically.
How do we seek consent to hold it	Voluntary anonymised equality and diversity forms provided at the end of courses for members to complete.
How do we record consent	As the forms are voluntary, and only completed by those who already complete an application form detailing SC's data protection policy, there is no additional requirement to complete a consent form. Electronic application form copies are saved on the shared drive, providing confirmation of consent.
How long we hold it for	From point that the form is submitted to the beginning of the month after the first anniversary of the date of attendance on course.
Process for deletion of records	At the beginning of each month, all forms relating to attendance on courses 12 months previously are deleted from database and equality and diversity monitoring form is deleted.

2.5 Personal details of those who work with the charity: Trustees, Council Members and Faculty

In order to work effectively as a charity, we need to ensure we can contact those who work closely with us.

What data we hold	This is variable but could include the following: • Name • Email address • Phone number • Home address • Job title • Organisation • Background • Photo of individual
Why we hold it	• So, we are able to contact those who work with the charity. • In order to comply with statutory regulations for reporting who our Trustees are. • So, we can share more widely details of those involved.
How we hold it	• Database of contact details are maintained and regularly updated as necessary. • Details of Trustees/Council Members and Faculty are shared on the charity's website and updated regularly.
How do we seek consent to hold it	Consent forms are provided to all new members to continue to hold data and to publish data on the website.
How we record consent	Electronic copies of all consent forms are saved on the SC shared drive.
How long we hold it for	Ongoing.
Process for deletion of records	Should a member decide to no longer work with the charity, they can request for their contact details to be deleted.

2.6 Bank details of those who provide paid services to the charity

In order to work effectively as a charity, we need to ensure we can pay those who provide non-voluntary services to the charity. In order to do this, we need to have banking details for those we need to pay. In order to comply with our statutory financial obligations, we must retain a copy of all financial records for 7 years from the end of the tax year within which the payment falls.

What data we hold	This is variable but could include the following: • Name • Email address • Phone number • Business address • Organisation • Invoice/expense claim details • Description of services provided and associated rates • Bank account details
Why we hold it	• So, we are able to pay for non-voluntary services. • In order to comply with statutory financial regulations for reporting to HMRC.
How we hold it	• Copy of all financial records are stored electronically. • Copy of some financial records may be held in paper form in a locked cupboard.
How do we seek consent to hold it	Consent forms are provided to all new claimants in order to be set up as a supplier for the charity.
How we record consent	Electronic copies of consent forms are saved on SC shared drive.
How long we hold it for	Ongoing.
Process for deletion of records	Should a supplier decide to no longer be a supplier for the charity, they can request that their contact details and financial records be deleted. However, for statutory reasons, this will not happen until 7 years after the end of the tax year within which the last payment was made.

3. Procedure for responding to subject access requests

3.1 Procedure for responding to subject access requests: when an individual requests a copy of information held about themselves.

Individuals have a right to understand the data that is held about them by an organisation. If an individual makes a request to see a copy of the record that SC holds for them then the charity will:

1. Acknowledge the individuals request by email within 48 hours of receiving the request.
2. Submit a copy of any paper or electronic records the charity holds within 30 days.

3.2 Procedure for responding to subject access requests: when an organisation requests a copy of information about one of their members of staff.

There may be occasions where it is necessary for an organisation to request a copy of records that the charity holds in relation to a member of staff. When individuals apply to attend a course with SC, they consent that SC can share identifiable details with a third party for the following two reasons only:

1. With the sponsor/organization of an individual member to confirm attendance on a course.
2. With the sponsor/organisation of an individual Member to organize the payment of course fees.

SC declares that it does not provide reports on individual performance to sponsors/organisations.

Where SC receives a request from an organisation in relation to their staff they will:

1. Acknowledge the request by email within 48 hours of receiving the request.
2. Consider the organisation's request and deem whether the request meets either of the two reasons SC declares it will share data for.
3. Where it is deemed to be an acceptable request, submit a copy of any paper or electronic records the charity holds within 30 days.
4. Where it is not deemed to be an acceptable request, the charity will advise the requester, via email/in writing, of the reason why they are unable to share the information requested, within 30 days.

3.3 Procedure for responding to subject access requests: when an individual or organisation requests a copy of information about someone else.

Where SC receives a request from an individual or organisation for information about someone else they will:

1. Acknowledge the request by email within 48 hours of receiving the request.
2. Consider the request and deem whether the request meets the criteria it has for sharing data. It may be possible under some circumstances to share identifiable data with a third party if they are acting on behalf of the individual concerned, e.g. where a

solicitor may request data on behalf of their client. In such cases, SC may contact the individual concerned for their consent to share data with a third party.
3. Where it is deemed to be an acceptable request, submit a copy of any paper or electronic records the charity holds within 40 days.
4. Where it is not deemed to be an acceptable request, the charity will advise the requester, via email/in writing, of the reason why they are unable to share the information requested, within 40 days.

4. Procedure for protecting individual rights

The charity protects individual rights by ensuring:

1. All individuals have a right of access to a copy of the information comprised in their personal data.
2. All individuals have a right to object to processing that is likely to cause or is causing damage or distress.
3. All individuals have a right to prevent processing for direct marketing.
4. All individuals have a right to object to decisions being taken by automated means.
5. All individuals have a right, in certain circumstances, to have inaccurate personal data rectified, blocked, erased or destroyed.
6. All individuals have a right to claim compensation for damages caused by a breach of the Act.

5. Procedure for deletion of records

The charity has a procedure whereby it reviews the records it holds on the first working day of every month. The following steps describe the process:

1. Check the SC Member Database for any training records with a deletion date listed in the past month.
2. Delete the application form (if applicable) for any individual with a record showing a planned deletion date for the past month.
3. Delete the consent form for any individual (if applicable) with a record showing a planned deletion date for the past month.
4. Check whether there are any other files on record relating to the individuals whose records show a planned deletion date of the past month and delete these.
5. Delete the Member training record from the SC Member Database.

6. How data protection is designed into systems

The charity has developed a number of systems in order to protect information.

Management and organisational measures

The charity carries out an annual information risk assessment to assess the types of data it holds, the sensitivity of this data and assesses the requirements for adequate security measures to protect it.

The charity has a designated Data Protection Officer who is responsible for ensuring that:

- Processes are in place to protect personal data and charity IT systems
- Personal data is only kept for the period of time it is needed for.
- Only staff members who require access to personal data have access.
- All staff members with access to personal data have appropriate training in how to use charity systems and awareness of their own responsibilities with regards to security issues.
- Ensuring there are appropriate business continuity arrangements in place that identify how to protect and recover any personal data the organisation holds.

Physical security

The charity's premise is protected by alarms, security lighting, CCTV and has a 24-hour security guard on the building's reception. The charity is hosted within the UK Health Forum's office. This is only accessible to members of UK Health Forum and SC. Visitors must be accompanied within the building at all times.
The charity has 2 lockable cupboards, with keys that are looked after by the COO at all times.

Computer security

The charity has taken various measures to protect data:

- The charity has virus protection software on all of its computers and laptops. Each of these is updated annually and the charity maintains a log of the expiration dates for each subscription.
- The charity ensures it is regularly updating all of its software as new updates come out.
- The passwords on all devices, both work provided and personal, that are used to access personal data, have new passwords on the first working day of every month. A log is maintained of the change in passwords.
- The charity keeps all of its documents on a cloud based system. Only those who require access to this system have it. The system is a double encrypted system so individuals need both a password to log into it, and to gone through an additional level of security to enable their device to work with it.
- Further security is provided on documents which include personal data with another password required for access to these.

Training of staff members

The most common reasons organisations have security breaches is due to a lack of security awareness and training for the individuals that work for them. As such the charity ensures that all of its members of staff receive regular training to ensure they understand:

- The most common threats to security.
- How hackers can get in to IT systems.
- Common scams and methods that hackers can deploy.
- Simple things individuals can do to reduce the chance of falling for a scam or leaving a system open for a hacker to exploit.

- The responsibility individuals have to ensure their working practices don't put IT systems at risk.
- What individuals need to do if they suspect that there might be a breach.
- Individuals responsibility to ensure their devices are protected and that passwords are updated regularly.

Cyber insurance

The charity has a comprehensive cyber insurance policy through its insurers, Hiscox. In the event of a data breach, the expert team at Hiscox would provide immediate support to the charity to:

- Reclaim any data that has been lost
- Minimise any potential damage to individuals through the loss of their data
- Notify all those involved that there has been a breach and the implications of this
- Provide pro-active advice to protect systems in the first place.

7. Procedure for dealing with a security breach

If, despite the security measures the charity has in place to protect the personal date it holds, a breach of security occurs, it is important that it deals with the security breach effectively. The breach may arise from a theft, a deliberate attack on your systems, from the unauthorised use of personal data by a member of staff, or from accidental loss or equipment failure.

In the event of a security breach the charity will:

1. Assess the scale of the breach, understanding what data has been compromised and whether it is recoverable. Assess the risks associated with the breach including any potential adverse consequences for individuals, how serious they are and how likely are they to happen.
2. Notify the charity's cyber insurers for support and advice on how to deal with the breach.
3. Put in place any procedures possible to contain the breach and recover any data lost.
4. Notify the Information Commissioners Officer (ICO), any other regulatory bodies, any third parties as deemed appropriate such as the police, banks and media.
5. Notify those who's data has been breached, explaining what has been accessed, the efforts taken to date to contain the breach and recover data and the plan in place to recover anything further.
6. Investigate the causes of the breach and evaluate the effectiveness of the response to it. Use the learning from these to inform any changes to policies and procedures going forwards.