GDPR Policy

These guidelines will be reviewed at least once a year.
Date of last review: March 2020

GDPR (General Data Protection Regulation) - BACKGROUND

GDPR came into force on the 25 May 2018 and replaced the Data Protection Act 1998. Regardless of the impact of Brexit, GDPR will remain. GDPR provides greater protection to individuals and places greater obligations on all organisations that process personal data about a Data Subject.

Scarf is required to keep certain information about its employees, trustees, volunteers, members, service users and other members of the public to enable us to provide the services we offer. It is also necessary to process information so that staff can be recruited and paid, activities organised and legal obligations to funding bodies and government fulfilled.

KEY PRINCIPLES

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this Scarf must comply with the General Data Protection Regulation (GDPR) (EU) 2018. In summary this states that personal data must be:

- Obtained and processed fairly and lawfully
- Obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose
- Adequate, relevant and not excessive for that purpose
- Accurate and kept up to date
- Not kept for longer than necessary
- Processed in accordance with the data subject's rights and consent
- Kept safe from unauthorised access, accidental loss or destruction
- Not be transferred to a country that does not have reciprocal arrangements to the UK, unless that country has equivalent levels of protection for personal data
- Data subjects have the right to request access to their personal information. The GDPR states that this should be responded to within one month.

GDPR does not apply to any personal data held about someone who has died. Both the Access to Medical Reports Act 1988 and the Access to Health Records 1990 will continue to apply.
All Scarf staff and Committee Members need to ensure the ways in which they handle personal

data meet the requirements of GDPR as outlined in Scarf's GDPR Policy. Staff and volunteers will have access to and have awareness of this policy, receive appropriate training where necessary, and be encouraged to seek further guidance where needed.

SCARF'S APPROACH TO GDPR

The requirements that Scarf need to meet vary depending on whether Scarf is a Data Controller or a Data Processor. We recognise that in most scenarios, Scarf will be a Data Controller and the organisation is therefore ultimately responsible for implementation.

Special categories of data attract a greater level of protection, and the consequences for breaching GDPR in relation to special categories of data (personal information of data subjects that is especially sensitive) may be more severe than breaches relating to other types of personal data.

Any member of staff, committee member/trustee or volunteer, who considers that this policy has not been followed in respect of personal data about him/herself, should raise the matter with Scarf's Committee. If the matter is not resolved it should be raised as a formal grievance. If a service user/individual is not happy with respect to our use of their personal data, they may refer to our Complaints Policy.

Scarf recognises that in addition to complying with the key principles, Scarf must be able to provide documentation to the Information Commissioner's Office (ICO) on request, as evidence of compliance. We understand that we must also adopt 'privacy by design'. Data protection should not be an after-thought.

INFORMATION HELD

Personal information is defined as any details relating to a living, identifiable individual. This applies to employees, committee members, trustees, volunteers, members, service users and other members of the public. This information may include an individual's name, postal, email and other addresses, telephone numbers, subscription details, organisational roles and membership status. In the case of service users, this will include school details, medical details and sensitive personal information.

Personal information is kept in order to enable Scarf to deliver services to its members and service users effectively and understand the history and activities of individuals or organisations within the voluntary and community sector.

Scarf must ensure that information relating to these people is treated correctly and with the appropriate degree of confidentiality.

Some personal information is defined as Sensitive Data and needs to be handled with special care. Sensitive information is defined by the Act as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment

purposes or to protect the vital interests of the person or a third party.

All employees, committee members/trustees, volunteers, members, clients and other members of the public have the right to:

- Know what information Scarf holds and processes about them and who holds it
- Know how to request access to it
- Know how to keep it up-to-date
- Know what Scarf is doing to comply with its obligations under the Act
- Know they have the right to request the removal/deletion of this information

PROCESSING PERSONAL DATA

Scarf must only process personal data if we are able to rely on one of a number of grounds set out in GDPR. The grounds which are most commonly relied on are:

- The Data Subject has given his or her consent to the organisation using and processing their personal data
- The organisation is required to process the personal data to perform a contract; and
- The processing is carried out in the legitimate interests of the organisation processing the data – note that this ground does not apply to public authorities

The other grounds which may apply are:

- The processing is necessary to comply with a legal obligation
- The processing is necessary to protect the vital interests of the Data Subject or another living person
- The processing is necessary to perform a task carried out in the public interest

All staff and volunteers who process or use any personal information are responsible for ensuring that:

- Any personal information which is held is kept securely and used for purposes specified; and
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party

Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct.

Personal information should be:

- Kept in a locked filing cabinet or in a locked drawer and used solely for the purpose for which it is intended
- If the information is computerised, should be password protected and kept as securely as possible
- If personal information is collected by telephone, callers should be advised what the information will be used for.

Disposal of confidential material:

- Sensitive material should be shredded. Particular care should be taken to effectively delete information from computer hard drives if a machine is to be disposed of or passed onto another member of staff.

Personal or confidential information should not be discussed in public areas or within open-plan office areas. In staff briefings at the start and end of activities (eg. youth club and multi sport club), staff should ensure others are not around or able to hear if personal or confidential information is being discussed.

All staff should be aware of the difficulties of ensuring confidentiality in an open or public area and respect the confidential nature of any information inadvertently overhead.

COLLECTING INFORMATION

Whenever information is collected about people, they should be informed why the information is collected, who will be able to access it and for what purposes it will be shared. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of Scarf.

Any notes taken during or after an interview should be relevant and appropriate. Such notes should be filed in a legible and coherent manner and information notes are retained for no longer than necessary in a secure place, before being shredded.

DATA RETENTION AND SECURITY

Two of the key principles of GDPR are data retention and data security.

Data retention refers to the period for which Scarf keeps the personal data that has been provided by a Data Subject. At a high level, Scarf must only keep personal data for as long as it needs the personal data. General information about clients (ie: members/service users) cannot be kept indefinitely unless there are specific requests to do so.

Scarf will also need to retain information about staff. In general all information will be kept for six years after a member of staff leaves the organisation. Some information however, will be kept for much longer, for example, if required by funders. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and information required for job references.

All staff are responsible for checking that any information they provide to Scarf in connection with their employment, is accurate and up-to-date. Staff have the right to request any personal information that is being kept about them either on computer or in manual filing systems by contacting Scarf's Chair.

Data security requires Scarf to put in place appropriate measures to keep data secure (as outlined above).

PUBLICATION AND USE OF SCARF INFORMATION

Scarf aims to make as much information public as is legally possible. In particular information about Scarf's staff, committee members/trustees and members will be used in the following circumstances:

- Scarf may obtain, hold, process, use and disclose information in connection with the administration, management and business activities of Scarf, including making and keeping lists of members and other relevant organisations
- Scarf may publish information about our organisations and its members including lists of members, by means of newsletters or other publications
- Scarf may provide approved organisations with lists of names and contact details of members or other relevant organisations only where the members or other relevant organisations have given their consent
- Names of, and a means of contacting staff and trustees, may be published within publicity leaflets and on the website.

DUTY TO DISCLOSE INFORMATION

There is a legal duty to disclose certain information, namely information about:

- Child abuse, which will be disclosed to relevant agencies/police
- Drug trafficking, money laundering or acts of terrorism or treason, serious assault, murder, which will be disclosed to the police.

WEBSITE PRIVACY POLICY & PROCEDURE

Where Scarf collects personal data via a website, we understand that we will need a GDPR compliant website privacy policy. The privacy policy explains how and why personal data is collected, the purposes for which it is used and how long the personal data is kept.

SUBJECT ACCESS REQUESTS

One of the key rights of a Data Subject is to request access to and copies of the personal data held about them by an organisation. Where Scarf receives a Subject Access Request, we understand that we will need to respond to the Subject Access Request in accordance with the requirements of GDPR, ie: usually within one month of the request.

THE RIGHTS OF A DATA SUBJECT

In addition to the right to place a Subject Access Request, Data Subjects benefit from several other rights, including the right to be forgotten, the right to object to certain types of processing and the right to request that their personal data be corrected by Scarf.

BREACH NOTIFICATION UNDER GDPR

We understand, that in certain circumstances, if Scarf breaches GDPR, we must notify the ICO and potentially any affected Data Subjects without undue delay. The report to the ICO must be done within 72 hours of becoming aware of the breach, where feasible.

TRANSFER OF DATA

If Scarf wishes to transfer personal data to a third party, we understand that we should put in place an agreement to set out how the third party will use the personal data. The transfer would include, for example, using a data center in a non-EU country. If that third party is based outside the European Economic Area, we recognise that further protection will need to be put in place and other aspects considered before the transfer takes place.

COMPLIANCE WITH GDPR

Compliance with GDPR is overseen in the UK by the ICO (www.ico.org.uk). Under GDPR, the ICO has the ability to issue a fine of up to 20 million Euros (approximately £17,000,000) or 4% of the worldwide turnover of an organisation, whichever is higher. The potential consequences are therefore significant.

Scarf appreciates that it is important to remember, however, that the intention of the ICO is to educate and advise, not to punish. The ICO wants organisations to achieve compliance. A one-off, minor breach may not attract the attention of the ICO but if Scarf persistently breaches GDPR or commits significant one-off breaches (such as the loss of a large volume of personal data, or the loss of special categories of data), it may be subject to ICO enforcement action. In addition to imposing fines, the ICO also has the power to conduct audits of Scarf and our data protection policies and processes. Scarf realizes that the ICO may also require Scarf to stop providing services, or to notify Data Subjects of the breach, delete certain personal data we hold or prohibit certain types of processing.

SUPPORTING THIS POLICY

Supporting this policy is our Privacy Statement which explains how Scarf approaches the issue of Data Protection. This can be found below and also on our website at www.scarfnewforest.org.

SCARF PRIVACY STATEMENT

Scarf is committed to keeping any personal data you share with us safe, we will be clear whenever we are collecting data why we are collecting it and ensure that we don't use your data for anything you wouldn't reasonably expect.

Information quality:

- We will ensure that the information about you is accurate and up-to-date when we collect or use it. You can help us with this by keeping us informed of any changes to the information we hold about you.

Information security:

- We will keep information about you in a secure manner and it will only be accessible to relevant Scarf staff
- We will protect your information against unauthorised change, damage, loss or theft

Keeping information:

- We will hold information about you only for as long as the law says. After this it will be disposed of securely and properly

Openness:

- We will tell you on request what kinds of information we hold and what we do with it.

Access and correctness:

- Whenever possible, we will let you see the information we hold about you and correct it if it is wrong

Sharing Information with others:

- Sometimes we have to confirm or share information with other organisations. If we need to do this, we will make it clear to you on the forms you complete
- We will draw up an agreement with the organisation that we need to share information when appropriate. This is to ensure that both parties understand why the information is being passed on and what use can be made of it. In some cases, a third party organisation such as a funding body may draw up the agreement.

In general:

- We will comply with the General Data Protection Regulations 2018 and any subsequent legislation on information handling and privacy
- We will do this through the Scarf GDPR Policy (available on our website www.scarfnewforest.org) and we will help you with any questions or problems that you may have
- If we cannot help you, we will give you advice on where you can access the relevant information

Our Commitment:

- We will only collect information that is necessary
- We will be fair in the way we collect information about you
- We will tell you who we are and what we intend to do with the information about you
- Where practicable, we will collect information directly from you
- If we collect information about you from someone else, we will make sure you know that we have done this, whenever possible.