

1. Why does FOCUS need a Data Protection Policy?

As FOCUS maintains records of the personal details of its staff members, volunteers, beneficiaries, donors and other individuals, this Data Protection Policy ensures that FOCUS is compliant with the General Data Protection Regulations (GDPR), 2018 and the Data Protection Act (DPA), 1998.

A brief outline of FOCUS' Data Protection Policy (Privacy Notice) is displayed in FOCUS' office, on FOCUS' website, and is made available to all 'data subjects'.

2. FOCUS Data Protection Statement

- 2.1 It is the policy of FOCUS to ensure that that personal data held by FOCUS about its employees, volunteers, beneficiaries, donors and other parties is obtained and processed fairly and lawfully. FOCUS takes all necessary steps to implement this Policy.
- 2.2 FOCUS regularly monitors relevant statutory legislation to keep its Data Protection Policy up-to-date. FOCUS also periodically monitors its procedures to ensure compliance with the Data Protection Policy.
- 2.3 FOCUS implements and complies with the eight principles underlying good conduct in processing personal information. These eight principles are:
 - a) Personal data is processed fairly and lawfully
 - b) Personal data is processed for limited purposes and is not further processed in any way that is inconsistent with the original reason for getting the data
 - c) Personal data is adequate, relevant and not excessive in relation to the purposes for which they are processed
 - d) Personal data is accurate and kept up to date
 - e) Personal data is kept no longer than is necessary
 - f) Personal data is processed in accordance with the subject's rights under the GDPR
 - g) Personal data is kept secure and protected against loss or damage
 - h) Personal data is adequately protected if transferred to countries outside the European Union
- 2.4 FOCUS asks for feedback from its staff on a regular basis to review the efficacy of the Data Protection Policy and to suggest improvements to its delivery and compliance.
- 2.5 FOCUS monitors the delivery and efficacy of the Data Protection Policy via an annual review.
- 2.6 The Chief Executive has overall responsibility for Data Protection Policy delivery.

3. Responsibilities of FOCUS employees and Trustees.

3.1 Chair of Trustees

The Chair of Trustees, in consultation with the Board of Trustees, approves the annual review of the Data Protection Policy and recommends any action resulting from the review.

The Chair of Trustees will have full access to all data as required to maintain effective communications with the board and staff team and in an emergency in the event of breach of data security

3.2 Chief Executive

The Chief Executive holds overall responsibility for ensuring that the Data Protection Policy is applied within the organisation as a whole. They perform an annual review to monitor and ensure compliance with the Data Protection Policy.

The Chief Executive has full access to all data in order to maintain and ensure compliance with this policy

3.3 Project Managers

Project Managers have responsibility for ensuring Data Protection Policy compliance within their projects. They have the responsibility of keeping any databases (either paper-based or computer-based) they maintain compliant with FOCUS Data Protection Policy. They will support the annual review, providing any required information or data to the Chief Executive. They also ensure that other staff and volunteers within their project are aware of the Data Protection Policy.

Project Managers have full access to the data generated within their projects in order that they can maintain effective communications with all beneficiaries, staff, volunteers and other related parties and to safeguard their welfare.

3.4 Office Co-ordinator

The Office Co-ordinator has responsibility for maintaining any financial or administrative records in a manner consistent with good practice outlined by the Data Protection Policy. The Finance & Administration Assistant maintains the annual review records and any matters arising from its delivery.

The Office Co-ordinator will have full access to staff personnel records as required to maintain these and to effectively manage payroll and pensions obligations.

3.6 Other Staff

Other staff will have responsibility for capturing personal and sensitive data of volunteers and beneficiaries of the project in which they are employed or of other persons involved with FOCUS in the case of administrative staff.

Other staff will have access to that information required to maintain accurate records of FOCUS' activities and to contact those persons who have requested that they be kept informed.

3.7 Trustees

Individual trustees who hold any personal or sensitive data at home are required to self-regulate to ensure compliance with the Data Protection Policy.

Trustees will not have access to personal data without the specific authority of the Chair of Trustees or an authorised body or agency.

4. Guidelines for delivery of FOCUS' Data Protection Policy

These follow the order of the eight principles of good practice outlined in section 2.

4.1 With respect to fair and lawful processing of personal data:

All FOCUS employees (and where appropriate volunteers) who either collect or process personal (including sensitive) data are to read and comply with this Data Protection Policy.

Personal data can be defined as any data that can aid in identifying a person. This includes:

- Factual information e.g. name and address
- Ethnic origin
- Religious or other beliefs*
- Physical and/or mental health*
- Criminal convictions (including allegations)*

*Items marked with an asterisk can also be considered to be sensitive data

To avoid unauthorised or unnecessary data being collected, only official FOCUS forms can be used to collect personal data.

A Data Lineage Map and accompanying Notes will be maintained illustrating how data is collected, handled, stored, accessed and destroyed.

All persons from whom data is requested must be made aware of FOCUS' Data Protection Policy using the Privacy Notice and their specific consent must be requested.

4.2 With respect to gaining and processing personal data for limited purposes:

Data is only collected for one reason on any given occasion. If the same data, once collected, is to be used for a different purpose the data subject must be informed and asked for consent.

It is acceptable to ask for consent to process personal data for other purposes when the data is first collected provided the data subject can clearly understand what those purposes might be.

When collecting the data the length of time for which it will be kept must be clearly stated.

4.3 With respect to personal data being adequate, relevant and not excessive in relation to the purposes for which they are processed:

When collecting data, only the types of data listed on the required standard form can be collected e.g. the referral form, medical form etc.

Data is not collected if it is only considered that it 'may be useful in the future'. However...

If data relating to the future has any bearing within the time-scale of a FOCUS event that the data subject is attending, e.g. a residential, then it is acceptable to collect that data, e.g. a possibility that a medication administration regime may change during an event thus necessitating a change of medication.

4.4 With respect to personal data being accurate and kept up-to-date:

Ensure that any notes taken are accurate e.g. a disclosure on a residential event. Confirm their accuracy by reading them back to the data subject.

If any forms are returned where the hand-writing is illegible, contact the subject and confirm exactly what was written.

If any changes to a subjects' personal records occur, e.g. address change, then the date of the change must be noted and it must be clear within all filing systems and databases which is the most up-to-date record.

4.4.1 Subject Access Requests:

If a data subject believes that information held about them is inaccurate, or they are concerned about how their data is being used, they may request to see it (or copies of it) in order that it be deleted or corrected.

Information requests will be free of charge to the data subject

Information may be withheld from a data subject if releasing it would reveal information about other data subjects and their permission is not granted for the information to be released.

4.5 With respect to data being kept for no longer than is necessary:

Records which FOCUS maintains are 'weeded' on an annual basis to remove any data that has been kept for the necessary length of time.

In line with our Retention Policy, the following retention periods will apply for all personal and sensitive data:

Type of Record	Length of Retention
Beneficiary Files (inc. application or referral forms, medical forms, consent forms)	For 3 years after their last involvement or until the beneficiary is 25 years of age , whichever is the longer
Safeguarding Records (inc. Incident Forms and Records of Disclosure)	Until age 100 of beneficiary. Note that the entire Beneficiary File will be retained in this case
Evaluation and Feedback Forms	For 3 years after the end of the project
Staff Personnel Files (inc. contracts, job history, references, medical forms and sickness record, payroll and pension records)	Until age 100
Staff Personnel Files (inc. review and supervision records, annual leave records, training history)	For 6 years after leaving date
Volunteer Files (inc. application forms, medical forms, references)	For 90 years after last involvement to account for any reference to in a Safeguarding Report
Individual Donor Details (inc. contact details and records of financial contributions)	For 7 years after their last donation

4.6 With respect to personal data being processed in accordance with the subject's rights under the GDPR 2018:

4.6.1 Data subjects have the right to...

- be informed about how their personal information will be processed
- have access to personal information held about them
- rectify any inaccurate information or data

- request erasure of personal information for which there is no compelling reason for retention
- restrict processing of personal information beyond what has been granted consent
- data portability for its reuse within another service or organisation
- object to processing of personal information that unfairly disadvantaged them
- not to be subject to automated decision-making including profiling

4.6.2 There are exceptions to the rights listed above, which are described in 4.4.1.

4.6.3 If FOCUS deems that dissemination of a certain piece of data is likely to cause physical or psychological harm to that person, FOCUS reserves the right not to give out that information

4.7 With respect to personal data being kept secure and protected against loss or damage:

All data kept in paper form must be kept in a locked location that is free of damp and away from potential fire damage.

During FOCUS residential events or when home-working, personal data recorded on paper must be kept in a locked box or cabinet, within a lockable office during residential events.

4.7.1 All data kept on computer:

Large databases e.g. Volunteer databases and Referrer databases are password protected if they are held on the computer hard drive.

Because FOCUS insurance policy requires weekly back-up of data stored on computer those back-up disks are kept in a secure and safe place away from damp and potential fire damage

If a FOCUS employee is processing personal data and a third party enters the office then that employee makes every effort to ensure that the data cannot be viewed.

When home-working, employees will make every effort to ensure that data cannot be viewed by other members of the household or visitors and will not leave computers or other devices 'unlocked' when not attended by the employee

The Chief Executive will keep a copy of any passwords in a locked location to which access will only be made in the event of emergency.

In line with FOCUS' IT, Online and Social Media Policy, secondary users of any staff member's work computer must use the 'Guest' log-in, from which access to sensitive or secure files cannot be gained.

4.8 With respect to personal data being adequately protected if transferred to countries outside the European Union (EU):

Information must only be transferred outside of the EU if the EU has determined that the level of protection for individuals will not be undermined by doing so.

5 Monitoring this policy

5.1 The Chief Executive reviews the Data Protection Policy annually and any changes (internal or statutory) in the requirements of the Policy, subsequently approved by the Board of Trustees, will be implemented.

- 5.2 In addition to the annual review of FOCUS' Data Protection Policy, the Chief Executive may make unannounced spot-checks to ensure compliance.
- 5.3 In the event of a breach of the GDPR, i.e. a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, where it is likely to result in a risk to the rights and freedoms of individuals, those individuals and the relevant supervisory authority will be informed within 72 hours of FOCUS becoming aware of the breach.
- 5.4 In addition to informing relevant authorities, in the event of a breach, the Chief Executive (or a nominated deputy) will inform the Chair of Trustees (or a nominated deputy) within 72 hours of becoming aware of the breach and will agree any actions required.

About us

FOCUS is a young people's charity. As such, we are required to hold certain information about the people we support and the people and organisations who support our work.

What information do we need to keep about you and why?

We only ask for and keep information about you that we need in order to ensure:

- You are kept informed about FOCUS' projects and events that may be of interest to you
- You are kept safe when involved in our projects and events
- We can keep track of who is involved with us and our work

This includes personal information such as your name, address, phone number and email address; and sensitive information such as medical details, dietary requirements or qualifications.

How we look after the information we keep about you

All personal or sensitive information that we hold about you will be kept in line with data protection law. This means that at FOCUS we will only keep personal or sensitive information about you for as long as is necessary. This includes the time you are actively involved and for a number of years afterwards, in line with good practice guidelines and our legal obligations.

What we do with the information we hold

We do not share any personal or sensitive information about you with anyone outside of FOCUS unless:

- Your (or another person's) welfare would be at risk if we did not
- We have your express permission to do so OR
- We are obliged by law to do so

Your rights

If at any point you believe that the information we hold about you is incorrect, you can request to see this information and have it corrected or deleted. If you wish to raise a complaint about how we have handled your personal information, you can contact us to have this investigated.

datacontroller@focus-charity.co.uk

If you are not satisfied with our response or believe that we have not used your personal information in line with the law you can complain to the Information Commissioner's Office


<https://ico.org.uk>

If at any point you would like to stop receiving information from us, you can email us at datacontroller@focus-charity.co.uk. Please write "Unsubscribe" in the Subject box. Alternatively, call us on 0116 251 0369. Although you are not required to provide a reason for this request, we would be grateful for any information you can provide so that we can improve our services.

Updating our policy

Each year Focus reviews its Data Protection Policy to ensure that it remains up-to-date with the latest legislation and that your rights are maintained.

The policy was last reviewed on: 17th May 2023

Signed:  _____

Matt Lilley, Chief Executive