Support for Young People Affected by Crime

Data Protection (GDPR) Policy

Context:

SAFE! is a charity that provides support to young people and families affected by crime, abuse and bullying in Oxfordshire, Berkshire, Buckinghamshire and Milton Keynes. SAFE! collects and records certain types of information about our service users. We may hold information on:

- Personal details of young people who are referred to our service for support including:
  - Name, address, DOB, ethnicity
  - Any special needs or mental health issues
  - Types of crime experienced
  - Behaviours
- Details of the support that we have provided to individuals

This information is used to provide the best possible service to individuals and to monitor and evaluate our service.

SAFE! also holds personal information on Employees, Sessional Practitioners, Students, Trustees and Volunteers and other professional business contacts.

SAFE! works in close partnership and cooperation with other agencies. In doing so, information about young people may need to be shared in order for them to get the most relevant and meaningful support as possible to help them recover. There should be justifiable reasons for the sharing of any information.

The individual's consent will always be sought before any information is shared, except where there is a significant safeguarding concern.

Legislation:

The Data Protection Act 2018 establishes rights and protection for individuals in relation to what information may be held about them and how it may be used. SAFE! fully endorses and adheres to article 5 of the GDPR which states that personal data should be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The Data Protection Act 2018 gives individuals the right to request a copy of any information held about them, this is known as a 'Subject Access Request'.

How we deliver our commitment to Data Protection:

SAFE! applies the Data Protection Act principles in relation to collection, use, retention, disclosure and disposal of information.

Information that includes personal data is stored on secure cloud-based servers (Office 365, the SAFE! Case Management System (CMS) and a shared database with Victim's First called Make Time Count(MTC)). Printed material is discouraged. Computers should be locked when staff are away from their desk and if Office 365/CMS/MTC is used from home, then no other person in that household should have access whilst in use. Likewise, any paper files kept at home between case visits should be safely stored in a locked cabinet.

Paperwork that is no longer required and containing confidential information is destroyed and disposed of by shredding.

Information held by SAFE! relating to individuals should only be discussed with other workers within SAFE! for example, in a supervision meeting, to gain advice or opinion from another worker or with another worker who may be jointly involved with the case. Only information which is relevant should be shared, and details should be discussed discreetly in a private room and not in front of others.

Personal information held by SAFE! will not be passed to any other agency without the person's consent unless:

- There is a legal obligation to disclose the information
- There are exceptional circumstances justifying a disclosure

SAFE! shall take reasonable steps to ensure that personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

SAFE!'s primary Data Controller is the CEO, Chloe Purcell.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, SAFE!' Data Controller shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

File Retention:

It is vital that information is appropriately managed and stored in line with Data Protection legislation, and that it is securely destroyed at the end of the designated retention period.
File retention principles are:

- To ensure that personal data is kept securely and not placed at risk of being lost or viewed by unauthorised persons
- To avoid unnecessary duplication of personal data and have procedures for safely sharing information electronically when appropriate
- To dispose of sensitive information securely at the end of the file retention period

- Logs are kept to ensure that data is destroyed in a timely fashion at the end of the required retention period

Data type	Required Retention Period
Electronic referrals and SAFE! Project Worker case records and evaluation forms, excluding anonymised records which may be retained for evaluation and research purposes.	Electronic service user data is stored between two systems. Some information is stored on the SAFE! IT case management system which is managed by a third party (Alberon) and stored in their secure servers. Some information is stored on the Victim First database Make Time Count (MTC) which is managed by a third party (Make Time Count). Case records and documentation are also stored on the secure cloud based server (Office 365). Any referrals where individuals have not consented to support should have personal details destroyed/deleted as soon as it is clear that they have not consented to support. All electronic records relating to individual cases are to be destroyed 10 years after the last contact in line with guidance from the NSPCC on retention of records. Project Workers should ensure records are uploaded to the case folder in the relevant office 365 drive and delete all records from their external data drive and SAFE! email account when they have completed the casework. This includes data stored on service databases as well as individual records. All service users have the right to request a copy of their records, and/or to ask that their records are deleted before the end of the ten-year period.
Paper referrals and SAFE! Project Worker case records and evaluation forms, excluding anonymised records which may be retained for evaluation and research purposes.	Paper files and records relating to SAFE! cases are discouraged as we have moved to a paperless system. Any historic paper records relating to individual cases are to be destroyed 10 years after the last contact in line with guidance from the NSPCC on retention of records.
Staff records including personal data, supervision notes, absence data, any disciplinary information etc.	All staff records are stored securely and confidentially on office 365. These will be stored for up to 6 years, and destroyed at the end of that period.

Related Policies:

Privacy Statement
Information Sharing Agreement (with Thames Valley Police)
Safeguarding Policy (Children)
Safeguarding Policy (Adult)
Complaints Policy

Further advice and Resources:

NSPCC guidance on records retention and storage
https://www.icmec.org/wp-content/uploads/2018/04/NSPCC-records-retention-and-storage.pdf

Further reading on the General Data Protection Regulation 2018
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Reviewing:

All policies are subject to an annual review and any additional regular review to reflect, for example, changes in legislation or to the structure of policies of SAFE!

Next Review due: October 2025