Charity No 900216

Supporting children and young people with disabilities and their families

Data Protection Policy

In line with the General Data Protection Regulation (GDPR)

Introduction

This policy applies to all staff and volunteers who handle or have access to personal data. There are a number of reasons why personal data is collected and retained by Forest Pulse, relating to members, children and young people attending activities, employees, volunteers and other stakeholders.

Through this policy we aim to ensure that members, employees, volunteers and stakeholders feel confident that we hold their data safely and responsibly. Failure to comply with data protection requirements when handling personal data is breaking the law. This can result in large fines and other legal sanctions. Data breaches can also cause significant distress to individuals and have an adverse impact upon the organisation's reputation. It is the responsibility of all staff or others who access or use personal information to adhere to this Data Protection Policy.

This policy should be read in conjunction with Forest Pulse Information Management & Security Procedures and Confidentiality Policy.

Purpose

The purpose of this policy is to:

- Define the requirements of the General Data Protection Regulation ("GDPR") as applied by UK Data Protection Legislation in the context of Forest Voluntary Action Forum.
- Clarify responsibilities and duties and set out the structure within which they will be followed.

Scope

This policy applies to all personal information processed by or on behalf of Forest Pulse.

The formats in which personal data is handled can range from electronic, hard copy, and voice recording formats, to spoken forms of communication.

Personal data is any information that can be attributed to an identifiable individual, including, but not limited to, names, email addresses, personal/medical history, academic performance, and qualifications.

Sensitive personal data or 'special category data' includes disability status, sexual orientation, sex life, ethnicity, medical information (both physical and mental health), political, philosophical, and religious opinions/beliefs, and details of criminal convictions or allegations. This category of data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls (e.g. a locked filing cabinet).

Other categories of data also require enhanced protection for example, bank details, other financial details, and national insurance numbers.

This policy also applies to de-identified (pseudonymised) personal data where individuals can be re-identified from other information.

Rights

All data subjects (an individual to whom personal data relates) have the following qualified rights:

- The right to rectification if the information held is inaccurate or incomplete
- The right to restrict processing and/or erasure of personal data
- The right to data portability
- The right to object to processing
- The right to object to automated decision making and profiling
- The right to complain to the Information Commissioner's Office (ICO)

In addition, individuals can request access to the personal data held about them. To access personal data held by Forest Pulse, an access to personal data form should be completed and sent to Kim Roberts, Data Protection Officer, by post or by email to charitymanager@forestpulse.co.uk

Obligations

To comply with the law, information must be collected and used fairly, stored securely, and not disclosed to any other person unlawfully. This is captured in the data protection principles set out in the GDPR. Those handling personal data must comply with these principles.

Personal data shall:

- Be obtained, processed, and used fairly, lawfully and transparently.
- Be collected for specified, explicit and legitimate purposes and not processed for any other purpose.
- Be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Be accurate and, where necessary, kept up to date.

- Be kept for no longer than is necessary.
- Be protected by appropriate security measures to prevent loss or unauthorised access.

In addition, personal data should not be transferred outside of the European Economic Area. In cases where this may be necessary, please seek the advice of the Data Protection Officer.

Privacy notices and lawful processing

Individuals must be provided with Privacy Notices when their personal data is collected or used. In some cases, Privacy Notices are already in place for the use of staff and volunteers' personal data. If you need something beyond this, please seek guidance from the Data Protection Officer.

Sharing of Information:

On occasion it may be necessary or beneficial to share information with other agencies, e.g. Education settings, Health, Social Care, or other agencies providing support to or becoming involved with the children/young people we support and their families, or on occasion our staff or volunteers. We will ask for consent to share this information where possible unless we are required to do so by law or to protect individuals from harm.

Third party data processing

Personal data cannot be processed by a third-party without the explicit consent of the data subject. In certain instances, where the relationship around data sharing is more complex, it may be necessary to agree a Data Sharing Agreement between the interested parties. Please contact the Data Protection Officer for advice.

Ad-hoc third-party requests for personal data (for example from the police) should be referred to the Data Protection Officer.

Data protection by design and default

It is the responsibility of all staff and volunteers to incorporate data protection by design and default into all activities, processes, or projects that may involve the use of personal data.

Personal data breaches

It is the responsibility of all staff and volunteers to immediately notify the Data Protection Officer by phone if you become aware that personal data is lost, misused, Compromised, or stolen. This includes, for example, the loss of a laptop. Where necessary, the Data Protection Officer will report breaches to the Information Commissioner's Office (ICO) and notify all individuals affected.

Deliberate misuse of personal data will result in disciplinary action and may lead to criminal prosecution. Examples of misuse include sharing passwords between colleagues, asking a colleague to give you data about a data subject or browsing data through unauthorised systems about data subjects. This list is not exhaustive.

Roles and Responsibilities

The Trustee Management Committee provide oversight of data protection matters within Forest Pulse.

The Data Protection Officer is the designated Forest Pulse contact for all matters related to data protection and first point of contact with the regulator (Information Commissioner's Office).

All staff are responsible for adhering to this policy as per the Terms & Conditions of employment.

Contact details for the Data Protection Officer are:

Kimberly Roberts,
Charity Manager, Forest Pulse.
Email charitymanager@forestpulse.co.uk. Tel: 01595-826357 /

Review

This policy shall be reviewed annually, or more frequently if appropriate, to reflect relevant legislative, regulatory, or organisational developments.

Signed

Pamela Jones, Chief Executive Officer
20.4.23