Policy
Data Protection

Policy	Reviewed	By whom?
Data Protection Policy	22/09/2025	Victoria Bacon

Next review date	15/09/2026
DSL	Leon Edwards
Contact details	leon@Pushforward.uk
	0330 8180186
Data Protection Officer	Victoria Bacon
Contact details	victoria@pushfoward.uk
Deputy Data Protection Officer	Francesca Ruiz
	francesca@Pushforward.uk

Policy Statement

Pushforward collects and uses information about people with whom it communicates.
This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the Data Protection Act 1998.

Pushforward regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain confidence between those with whom it deals.

To this end Pushforward fully endorses and adheres to the Principles of Data Protection, as set out in the Data Protection Act 1998.

Purpose

The purpose of this policy is to ensure that the staff and volunteers of Pushforward are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

Failure to adhere to the Data Protection Act 1998 is unlawful and could result in legal action being taken against Pushforward or it's staff and volunteers

Principles

The Data Protection Act 1998 regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Policy
Data Protection

Data users must comply with the data protection principles of good practice which underpin the Act. 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 Pushforward follows the eight Data Protection Principles outlined in the Data Protection Act 1998, which are summarised below:

I. Personal data will be processed fairly and lawfully
II. Data will only be collected and used for specified purposes
III. Data will be adequate, relevant and not excessive
IV. Data will be accurate and up to date
V. Data will not be held any longer than necessary
VI. Data subject's rights will be respected
VII. Data will be kept safe from unauthorised access, accidental loss or damage
VIII. Data will not be transferred to a country outside the European Economic Area, unless that
1. country has equivalent levels of protection for personal data.

The principles apply to "personal data" which is information held on computer or in manual filing systems from which they are identifiable. Pushforward employees, volunteers and trustees who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

Procedures

The following procedures have been developed in order to ensure that Pushforward meets it's responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by Pushforward falls into 2 broad categories:

1. Pushforward internal data records;
Staff, volunteers

2. Pushforward external data records;
Clients, students.

Pushforward as a body is a DATA CONTROLLER under the Act, and the Directors are ultimately responsible for the policy's implementation.

Internal data records

Policy
Data Protection

Purposes

Pushforward obtains personal data (names, addresses, phone numbers, email addresses), application forms, and references and in some cases other documents from staff and volunteers This data is stored and processed for the following purposes:

- Recruitment
- Equal Opportunities monitoring
- Volunteering opportunities
- To distribute relevant organisational material e.g. meeting papers, reports
- Payroll

Access

The contact details of staff and volunteers will only made available to other staff and Volunteers through an end to end encrypted Whatsapp Group/3CX/OneDrive. Any other information supplied on application will be kept in a secure filing cabinet and is not accessed during the day to day running of the organisation.

Group Development Resources

Contact details of staff, volunteers and trustees will not be passed on to anyone outside the organisation without their explicit consent.

A copy of staff and volunteer emergency contact details will be kept in the Emergency File for Health and Safety purposes to be used in emergency situations e.g. fire/ bomb evacuations.

Staff and volunteers will be supplied with a copy of their personal data held by the organisation if a request is made.

All confidential post must be opened by the addressee only.

Accuracy

Pushforward will take reasonable steps to keep personal data up to date and accurate.
Personal data will be stored for 6 years after an employee or volunteer has worked for the organisation and brief details for longer. Unless the organisation is specifically asked by an individual to destroy their details it will normally keep them on file for future reference. The Director has responsibility for destroying personnel files.

Storage

Policy
Data Protection

Personal data is kept in paper-based systems and on a password-protected computer system. Every effort is made to ensure that paper-based data are stored in organised and secure systems. (Office, locked cupboard)

Pushforward operates a clear desk policy at all times.

Use of Photographs

Where practicable, Pushforward will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisations website or in the Newsletter.

CCTV

Each unit of Pushforward contact CCTV cameras which record both audio and visual. (Please refer to our CCTV Policy for full details). Pushforward uses CCTV to protect the Company's property and to provide a safe and secure environment for employees, young people and visitors to the company's premises.

The data collected from the system will assist in a number of security measures including:

- Prevention or detection of crime or malpractice
- Identification and prosecution of offenders
- Monitoring the security of the our premises and equipment
- Ensuring that Health & Safety rules and company procedures are complied with
- Identification of unauthorised actions or unsafe working practices that might result in disciplinary investigations and to assist in providing relevant evidence
- Promoting productivity and efficiency
- The safety and welfare of our young people
- The safety and welfare of our staff, subcontractors and visitors

We will only collect and retain CCTV footage and Secure Cloud Recordings are deleted after 30 days. Recordings will only be kept as long as necessary for the purpose for which it was collected.

External data records

Purposes

Pushforward obtains personal data (such as names, addresses, and phone numbers) from Young people, families, carers and professionals working with the young people. This data is obtained, stored and processed solely to assist staff and volunteers in the efficient running of services. Personal details supplied are only used to send material that is potentially useful. Most of this information is stored on the organisation's database.

Policy
Data Protection

Pushforward obtains personal data and information from young people, families, carers and other professionals work with the young people in order to provide services. This data is stored and processed only for the purposes outlined in the agreement and service specification signed by the client/ member.

Consent

Personal data is collected over the phone and using other methods such as e-mail. During this initial contact, the data owner is given an explanation of how this information will be used.
Written consent is not requested as it is assumed that the consent has been granted when an individual freely gives their own details.

Personal data will not be passed on to anyone outside the organisation without explicit consent from the data owner unless there is a legal duty of disclosure under other legislation, in which case the Director will discuss and agree disclosure. Contact details held on the organisation's database may be made available to groups/ individuals outside of the organisation. Individuals are made aware of when their details are being collected for the database and their verbal or written consent is requested.

Access

Only the organisation's staff and volunteers will normally have access to personal data. All staff, and volunteers made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.

Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service through a password protected system.

Information will not be passed on to anyone outside the organisation without their explicit consent, excluding statutory bodies e.g. the Inland Revenue.

Individuals will be supplied with a copy of any of their personal data held by the organisation if a request is made.

All confidential post must be opened by the addressee only.

Accuracy

Pushforward will take reasonable steps to keep personal data up to date and accurate.
Personal data will be stored for as long as the person uses our services and normally longer. Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed according to the schedule in Appendix B. However, unless we are specifically asked by an individual to destroy their details, we will normally keep them on file for future reference.

Policy
Data Protection

If a request is received from an organisation/ individual to destroy their records, we will remove their details from the database and request that all staff holding paper or electronic details for the organisation destroy them. This work will be carried out by the Information Officer.

This procedure applies if Pushforward is informed that an organisation ceases to exist.

Storage
Personal data may be kept in paper-based systems and on a password-protected computer system. Paper-based data are stored in organised and secure systems.
Pushforward operates a clear desk policy at all times.

Use of Photographs
Where practicable, Pushforward will seek consent of members/ individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on the organisation's website or in the Newsletter.

Criminal Records Bureau
Pushforward will act in accordance with the CRB/DBS code of practice.
Copies of disclosures are viewed and a copy of the DBS number is kept on our electronic signal central record. In most cases this is no longer than 6 months in accordance with the CRB Code of Practice. There may be circumstance where it is deemed appropriate to exceed this limit e.g. in the case of disputes.

Responsibilities of staff and volunteers
During the course of their duties with Pushforward , staff and volunteers will be dealing with information such as names/addresses/phone numbers/e-mail addresses of members/clients/volunteers. They may be told or overhear sensitive information while working for Pushforward. The Data Protection Act (1988) gives specific guidance on how this information should be dealt with. In short to comply with the law, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Staff, paid or unpaid must abide by this policy.

To help staff and volunteers meet the terms of the Data Protection Act; the attached Data Protection/Confidentiality statement has been produced. Staff and volunteers are asked to read and sign this statement to say that they have understood their responsibilities as
part of the induction programme.

Compliance

Compliance with the Act is the responsibility of all staff, paid or unpaid. Pushforward will regard any unlawful breach of any provision of the Act by any staff, paid or unpaid, as a serious matter which will result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.

Policy
Data Protection

Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the line manager.

Retention of Data

Documents will be stored on secure electronic system for a period of 12 months and will then be deleted.
No documents will be stored for longer than is necessary.
All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.

ICO
As a registered member of the Information Commissioners Office we follow the expectations for CCTV as per their advice and guidance.

https://icosearch.ico.org.uk/s/redirect?collection=ico~sp-search&url=https%3A%2F%2Fico.org.uk%2Ffor-organisations%2Fuk-gdpr-guidance-and-resources%2Fcctv-and-video-surveillance%2F&auth=XPnO5kQZoinbT0McErmu0w&profile=_default&rank=1&query=cctv+policy