Data Protection and GDPR Policy

The Positive Impact Group

Effective Date
June 2026

Review Date
June 2027

Introduction

This policy is intended to clarify the obligations of The Positive Impact Group under the Data Protection Act 2018 (“the Act”) and the General Data Protection Regulation (GDPR). Everyone has rights with regard to how their personal information is handled. During the course of our activities, we will collect, store and process personal information about a number of different groups of people, and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, pupils, parents, trustees, governors, volunteers, suppliers and other individuals that we communicate with. The information, which may be held on paper, on a computer or other media, is subject to certain legal safeguards specified in the GDPR and the Act and other regulations, which impose restrictions on how we may use that information.

Scope

This policy shall apply in its entirety to all employees, including staff, agency workers, contractors, governors and volunteers who shall be referred to in this policy as “staff”.

In this policy, “school” means any of the settings within the organisation.

This policy does not form part of any employee's contract of employment, and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action. Breach of the GDPR or the Act may expose the Trust to enforcement action by the Information Commissioner or fines. Furthermore, certain breaches can give rise to personal criminal liability for the organisation’s employees.

All staff must read this policy carefully and make sure that they understand it.

Definition of Terms

Data is information which is stored electronically on a computer or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data on its own or when taken together with other information. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a school report) and can include telephone numbers, photographs and CCTV images.

Data controllers are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The organisation and the schools are the data controllers of all personal data used in the organisation.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves the use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Special categories of personal data include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic or biometric data, physical or mental health or condition or sexual life and sexual orientation. Special categories of personal data can only be processed under strict conditions. Data about criminal convictions and offences are not included under the definition of special categories of personal data, but similar safeguards apply and therefore for the purposes of this policy are treated in the same way.

Data Protection Principles

Anyone processing personal data must comply with the six Data Protection Principles. These provide that personal data must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date;
- not be kept longer than necessary for the purposes for which it is processed;
- be processed securely.

Fair and Lawful Processing

The GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be provided with certain information, including who the data controller is (in this case the organisation), the purpose for which the data is to be processed by us and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When special categories of personal data are being processed, more than one condition must be met. In some cases, the data subject's explicit consent to the processing of such data will be required.

Fair and lawful processing of data includes having legitimate grounds for collecting and using the personal data, not using the data in ways that have unjustified adverse effects on the individuals concerned, being transparent about how you intend to use the data and handling personal data only in ways they would reasonably expect.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at least annually afterwards. Inaccurate or

out-of-date data should be destroyed. If a data subject informs the organisation of a change of circumstances, their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the organisation will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the relevant Local Governing Body for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until the ' challenged ' marker is resolved, it will remain, and all disclosures of the affected information will contain both versions of the information.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required, in accordance with our data retention schedules.

Processing in Line with Data Subject's Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- request access to any data held about them by a data controller;
- object to processing based on legitimate interests, the performance of a task in the public interest, for direct marketing purposes or the purposes of scientific or historical research and statistics;
- ask to have inaccurate data amended, completed (if it is incomplete) or erased;
- ask for their personal data to be moved, copied or transferred from one IT environment to another in a safe and secure way;
- request the restriction or suppression of their personal data.

Data subjects also have certain rights in relation to automated decision-making, including profiling. We do not currently use automated decision-making in any of our processing activities. Some of the rights described above are not absolute and will be subject to, amongst other things, the legal basis for processing the personal data. A data subject can exercise these rights by contacting the Data Protection Manager, David Strong.

Data Security

The organisation has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The GDPR and the Act require us to put in place procedures to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if s/he needs it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- **Physical Security:** Appropriate building security measures are in place, and only authorised persons are allowed in the computer rooms. Disks, tapes, hard drives, memory sticks and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.
- **Computer Security:** Only authorised users are allowed access to computer files, and password changes are regularly undertaken. Computer files are backed up regularly. Data users should ensure that individual monitors do not show confidential information to passers-by and that s/he logs off from their PC when it is left unattended.
- **Procedural Security:** In order to be given authorised access to the computer systems, staff will have to undergo checks and will sign a confidentiality agreement. Staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source

documents are shredded before disposal. CDROMs and portable drives are physically destroyed when they are no longer required.

Dealing with Subject Access Requests

The GDPR extends to all data subjects a right of access to their own personal data. A request from a data subject for information that we hold may be received verbally or in writing. A fee cannot be charged for the provision of this information except in certain limited circumstances. Any member of staff who receives a written request should forward it to the Director immediately, as there are statutory time limits for responding (currently one month).

In order to ensure that people receive only information about themselves, it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the organisation's policy is that:

- Requests from pupils who are considered mature enough to understand their rights will be processed as any subject access request as outlined below, and the copy will be given directly to the pupil. The Information Commissioner's guidance is that it may be reasonable to adopt a presumption that by the age of 12, a child has sufficient maturity to understand their rights and to make an access request themselves if s/he wishes. In every case, it will be for the school to assess on behalf of the Trust whether the child is capable of understanding their rights under the Act and the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf.
- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent unless the school considers the child to be mature enough to understand their rights, in which case the school shall ask the child for their consent to disclosure of the personal data (subject to any enactment which permits the School to disclose the personal data to a parent without the child's consent). If consent is not given to disclose, the school shall not disclose the personal data if to do so would breach any of the data protection principles.

Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry will be made in the school's Subject Access log book, showing the date of receipt, the data subject's name, the name and address of

requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information. Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Providing Information Over the Telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the organisation. In particular s/he should:

- check the caller's identity;
- suggest that the caller put their request in writing;
- refer the request and the caller's identity details to the Data Protection Compliance Manager or the Head for assistance.

Authorised Disclosures

The organisation will only disclose data about individuals where it has identified a legal basis for doing so. The legal basis for processing personal data is set out in the relevant privacy notices provided to staff and pupils/parents.

Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the schools by staff will only be made available where the person requesting the information is a professional legitimately working within the organisation who needs to know the information in order to do their work.

CCCTV

The organisation may use CCTV in locations around its sites. This is to:

- safeguard pupils and staff;
- protect the school buildings and their assets;
- increase personal safety and reduce the fear of crime;
- support the Police in a bid to deter and detect crime;
- assist in identifying, apprehending and prosecuting offenders;

- protect members of the public and private property;
- assist in managing the schools.

Enquiries

General information about the Act can be obtained from the Information Commissioner's Office, www.ico.gov.uk.

Useful References:

- The Data Protection Act 2018
- The General Data Protection Regulation

Complaints

If you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with the relevant Data Protection Compliance Manager, David Strong: david.strong@positive-impactuk.com.

This policy is reviewed annually.

Overall responsibility lies with the Director, who liaises with the Senior Leadership Team to ensure a robust and sustainable model of Leadership.

Signed by Director

James Armson