GDPR Policy

AFFINITY 2020 CIC

|  |  |
| --- | --- |
| Date | February 17th 2020 |
| Written | C Elliott |
| Adopted | February 17th 2020 |
| Reviewed | February 17th 2021 2022 2023 2024 2025 |

1. **Aims**

Our organisation aims to ensure that all personal data collected about staff, young people, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1. **Legislation and guidance**

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) on the GDPR and the ICO’s code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. (should this be used at our permanent site)

It also reflects the ICO’s code of practice for the use of surveillance cameras and personal information.

1. Definitions Term Definition Personal data

Any information relating to an identified, or identifiable, individual. This may include the individual’s:

* Name (including initials)
* Identification number
* Location data
* Online identifier, such as a username It may also include factors specific to the individual’s physical, physiological, genetic, mental, economic, cultural or social identity.

Examples of personal data processed in the Organisation: Sign In - to facilitate the sharing of service users, staff and visitor information between sites and for the purpose of fire evacuation.

Special categories of personal data

Personal data which is more sensitive and so needs more protection, including information about an individual’s:

* Racial or ethnic origin
* Political opinions
* Religious or philosophical beliefs
* Trade union membership
* Genetics
* Sex life or sexual orientation

Examples of special categories of personal data processed in the Organisation: NHS and the Local authority will have access to health data for individuals and would hold medical records.

Processing Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

For example, by creating a service user record.

Data subject: The identified or identifiable individual whose personal data is held or processed.

Data controller: A person or organisation that determines the purposes and the means of processing of personal data.

Data processor: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

1. Roles and responsibilities

This policy applies to all staff employed within the organisation, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

* 1. Directors

The Directors have overall responsibility for ensuring that the organisation complies with all relevant data protection obligations.

* 1. Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the organisation processes, and for the ICO.

Full details of the DPO’s responsibilities are set out on the ICO website https://ico.org.uk/

* 1. CEO

The CEO acts as the representative of the data controller on a day-to-day basis.

* 1. All staff

Staff are responsible for:

* + - Collecting, storing and processing any personal data in accordance with this policy
    - Informing the organisation of any changes to their personal data, such as a change of address
    - Contacting the DPO in the following circumstances: With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure. If they have any concerns that this policy is not being followed. If they are unsure whether or not they have a lawful basis to use personal data in a particular way.If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area. If there has been a data breach. Whenever they are engaging in a new activity that may affect the privacy rights of individuals o If they need help with any contracts or sharing personal data with third parties

1. The data controller

Our organisation processes personal data relating to young people, staff, directors, visitors and others, and therefore the organisation is a data controller.

The organisation is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

1. Data protection principles

The GDPR is based on data protection principles that the organisation must comply with. The principles say that personal data must be:

* Processed lawfully, fairly and in a transparent manner
* Collected for specified, explicit and legitimate purposes
* Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
* Accurate and, where necessary, kept up to date
* Kept for no longer than is necessary for the purposes for which it is processed
* Processed in a way that ensures it is appropriately secure This policy sets out how Affinity 2020 CIC aims to comply with these principles.

1. Collecting personal data
   1. Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

* + - The data needs to be processed so that the organisation can fulfil a contract with the individual, or the individual has asked the organisation to take specific steps before entering into a contract
    - The data needs to be processed so that the organisation can comply with a legal obligation
    - The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life
    - The data needs to be processed so that the organisation, as a public authority, can perform a task in the public interest, and carry out its official functions
    - The individual (or their service user when appropriate) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

* 1. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to individuals when we first collect their data and will provide privacy notices to staff, young poeple to explain these reasons when data is first collected.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the organisations Information and Records Retention Policy.

1. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

* There is an issue with a service user that puts the safety of our staff at risk
* We need to liaise with other agencies and will only do this if compliant with Data Protection law.
* Our suppliers or contractors need data to enable us to provide services to our staff and young people – for example, IT companies.

When doing this, we will:

Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

Any request to share data, individuals to discuss with their line manager or Data Protection Officer for guidance.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

* The prevention or detection of crime and/or fraud
* The apprehension or prosecution of offenders
* The assessment or collection of tax owed to HMRC
* In connection with legal proceedings
* Where the disclosure is required to satisfy our safeguarding obligations
* Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided. We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our young people or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

1. Subject access requests and other rights of individuals
   1. Subject access requests

A subject access request (SAR) is a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under General Data Protection Regulations. The request does not have to be in a particular form.

If staff receive a subject access request they must immediately forward it to the DPO, we will then follow the procedure set out in the organisations GDPR Internal Procedures document. Reporting requirements will be managed centrally.

* 1. Young people and subject access requests

Personal data about a young person belongs to that young person, and not the family or other professionals. For a family or other professional to make a subject access request with respect to the young person, the young person must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

* 1. Responding to subject access requests

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

* 1. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

* + - Withdraw their consent to processing at any time
    - Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
    - Prevent use of their personal data for direct marketing
    - Challenge processing which has been justified on the basis of public interest
    - Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
    - Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
    - Prevent processing that is likely to cause damage or distress
    - Be notified of a data breach in certain circumstances
    - Make a complaint to the ICO
    - Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

1. CCTV (Ring Door Bell) (Jan 2024 update)

We use CCTV in various locations around the site we higher ensure it remains safe. We will adhere to the ICO’s code of practice and the company we higher forms CCTV policy for the use of CCTV.

We do not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use at the sights we higher.

Any enquiries about the CCTV system should be directed to the manager.

1. Photographs and videos

As part of our organisation activities, we may take photographs and record images of individuals within our programmes.

We will obtain written consent from young people or social care professionals for photographs and videos to be taken for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used.

When using photographs and videos in this way we will not accompany them with any other personal information about the service user, to ensure they cannot be identified.

1. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

* + Appointing a suitably qualified DPO organisation, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
  + Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
  + Completing privacy impact assessments where the organisations processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
  + Integrating data protection into internal documents including this policy, any related policies and privacy notices
  + Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
  + Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
  + Maintaining records of our processing activities, including:

For the benefit of data subjects, making available the name and contact details of our academies and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

1. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

* + Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
  + Papers containing confidential personal data must not be left on office, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
  + Where personal information needs to be taken off site, staff must sign it in and out from the office
  + Passwords that are at least 8 characters long containing letters and numbers are used to access office computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
  + Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
  + Staff who store personal information on their personal devices are expected to follow the same security procedures as for organisation owned equipment (see our ICT Acceptable Use policy.)
  + Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

1. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the academy’s behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

1. Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The organisation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in the organisations GDPR Internal Procedures document. Reporting requirements will be managed centrally.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in the organisations context may include, but are not limited to:

* + Safeguarding information being made available to an unauthorised person
  + The theft of the organisation’s laptop containing non-encrypted personal data about pupils

It should be noted that a breach of General Data Protection Regulation Policy could result in disciplinary action.

1. Training

All staff, are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school’s processes make it necessary.

1. Monitoring arrangements

The DPO organisation is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school’s practice. Otherwise, or from then on, this policy will be reviewed annually and shared with the board.