56-60 Nelson Street
London
E1 2DE
T: +44 2070 183700
M: info@i-access.uk
W: www.i-access.uk

GDPR and Data Protection Policy

Aim

Kilberry Computing Ltd. trading as iAccess aims to ensure that all personal data collected about staff, learners, 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.

Legislation

This policy meets the requirements of the GDPR and the expected provisions of the GDPR and 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 also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Definitions

Personal data

Any information relating to an identified, or identifiable, individual and includes the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as username

Special categories of personal data Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina
- and iris patterns), where used for
- identification purposes
- Health – physical or mental
- Sex life or sexual orientation

Processing

Anything done to personal data, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying

Data subject

The identification of, or identifiable, individual whose personal data is held or processed

56-60 Nelson Street
London
E1 2DE
T: +44 2070 183700
M: info@i-access.uk
W: www.i-access.uk

Data controller
A person or organisation that determines how and why personal data is processed

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, unauthorized disclosure of, or access to personal data

1. Introduction

IAccess processes personal data relating to employees, learner clients, visitors and others to allow us to monitor performance e.g. appraisals, achievements, and health and safety, for example, and is therefore a data controller. iAccess is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. It is also necessary to process information in order to recruit and pay staff, organise courses and comply with legal obligations to funding bodies and government. 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, iAccess must comply with the Data Protection Principles which are set out in the GDPR and DPA (2018).

In summary these state that personal data must be:

- obtained and processed fairly, lawfully and in a transparent manner
- collected for specified, explicit and legitimate purposes and shall not be processed in any manner incompatible with that purpose
- 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, kept safe from unlawful or unauthorised access, accidental loss, damage or destruction
- where we transfer data to a country outside the European Economic Area, we will do so in accordance with data protection law

Status

This policy does not form part of the formal contract of employment. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the DPO initially. If the matter is not resolved it should be raised as a formal grievance**.**

Designated 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 will provide an annual report of the activities directly to the

56-60 Nelson Street
London
E1 2DE
T: +44 2070 183700
M: info@i-access.uk
W: www.i-access.uk

SMT. 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 in their job description.

ALL STAFF

Staff is responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing iAccess 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 reply on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer data
    - If there has been a data breach
    - Whether they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Collecting Data

We will only process data where we have one of six '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 iAccess to take specific steps before entering into a contract
- The data needs to be processed so that the iAccess can comply with a legal obligation
- The data needs to be processed to ensure vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the iAccess, can perform a task
- The data needs to be processed for the legitimate interests of the iAccess or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or the parent/guardian/carer 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 data which are set out in the GDPR and DPA 2018

Limitation

We will only process data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

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.

56-60 Nelson Street
London
E1 2DE
T: +44 2070 183700
M: info@i-access.uk
W: www.i-access.uk

When staff no longer needs the personal data they hold, they must ensure it is deleted or anonymised.

Sharing Personal Data

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

- There is an issue that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and learners
- 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 data safe while working for us

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, mental health and special educational need (SEN) 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 pupils or staff.

iAccess will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. iAccess will only use the information in the protection of the health and safety of the individual.
iAccess office and training facility do not pose a threat or danger to other users. Therefore, all staff and learners will be asked to sign consent to process declaration, regarding particular types of information, when an offer of employment or a course place is made.

Access request

Individuals have a right to make a 'access request' to gain access to personal information that the organisation holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine

56-60 Nelson Street
London
E1 2DE
T: +44 2070 183700
M: info@i-access.uk
W: www.i-access.uk

this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the
- significance and consequences of this might be for an individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

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 or classroom desks, 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, numbers and special characters are used to access computers, laptops and other electronic devices and removable media, such as laptops and USB drives
- Encryption software is used to protect all portable devices and removable media such as laptops and USB drives
- Staff, pupils or others who store personal information on their personal devices are expected to follow the same security procedures as for iAccess-owned equipment
- 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
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

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 or incinerate paper-based records, and overwrite or delete electronic files.

56-60 Nelson Street
London
E1 2DE
T: +44 2070 183700
M: info@i-access.uk
W: www.i-access.uk

We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

iAccess will make all reasonable endeavours to ensure that there are no personal data breaches.
In the unlikely event of a suspected data breach, on finding or causing a breach, the staff member or data processor must immediately notify the DPO. When appropriate, we will report the data breach, to the ICO within 72 hours.

Processing of Sensitive Information

Sometimes it is necessary to process information about a person's physical health, details of criminal convictions, racial or ethnic origin, political opinions, religious beliefs, trade union activities, sexual life, or details of mental health. This may be to ensure iAccess is a safe place for everyone. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for iAccess to do this. More information on specific cases about this is available from the data protection officer, your head of department, the personnel department or the student services office.

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 iAccess processes make it necessary.

Conclusion

Compliance with the 2018 Act is the responsibility of all members of iAccess. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to organisation facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the data protection officer.

Review

The DPO is responsible for monitoring and reviewing this policy annually and report to
Kilberry Computing Ltd. trading as iAccess Management Team
GDPR and Data Protection policy 0.3