Data Protection Policy

Introduction

Open Awards is committed to the protection of all personal and sensitive data and to ensuring that the rights and privacy of individuals from whom we collect data Is protected in accordance with the Data Protection Act and General Data Protection Regulation (GDPR) May 2018. We fully endorse and adhere to the seven Principles of data protection as set out in the GDPR.

Open Awards collects and use certain types of information about people with whom it conducts business, in order to operate and fulfil its business functions. This policy sets out how we handle the Personal Data we collect which includes data about employees (current, past and prospective), customers, learners, suppliers, Board and Committee members and other third parties including data we may be required by law to collect to comply with the requirements of government departments. It also sets out what we expect from employees in order for Open Awards to comply with applicable law.

This policy applies to all Personal Data we process regardless of how it is collected, recorded and used – whether on paper, electronically, or other media on which data is stored.

Open Awards is committed to fulfilling our obligations under the data protection legislation as to the processing of personal data used in its business and in so doing meeting the expectations of employees and any other individual whose personal data we process. We regard the lawful and correct treatment of this data as very important to our successful operations, and to maintaining confidence between Open Awards and those with whom we carry out business.

Data Controller - Open Awards is the Data Controller and the Director of Corporate Services is responsible for overseeing this policy, with delegated authority to the Information Systems Officer. All staff must treat personal data in a confidential and secure manner and follow the guidance set out in this policy. Managers are responsible for ensuring staff comply with this policy and we will ensure that all employees have access to appropriate training relating to data protection. Any data breaches must be reported immediately to the Information Systems Officer as all breaches must be recorded and where necessary reported to the Information Commissioners Office (ICO).

Compliance - The requirements of this policy are mandatory and all Open Awards staff must read, understand and comply with this policy when processing personal data on our behalf. Failure to comply with company policy may result in disciplinary action, which could result in summary dismissal. You may also face criminal liability in certain circumstances.

This policy (together with related policies listed below (excluding learner and general Privacy Notices) is an internal document and should not be shared with customers or third parties without prior authorisation from the Information Systems Officer, Director of Corporate Services or CEO.

Notification

We are registered with the Information Commissioner's Officer (ICO) for processing of personal data and this is reviewed periodically by our Information Systems Officer Our notification number is Z9241641, if you are unsure whether a purpose for which you are processing data is covered by the notification you should check with the Information Systems Officer before continuing.

The main purposes for which we are covered under our notification include:

- personal details
- family, lifestyle and social circumstances
- financial details
- employment and education details
- goods or services provided

and sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- trade union membership

Processing personal data

Staff are processing personal data through actions such as inputting, altering, deleting, accessing, downloading, reviewing or transferring data whether it is a manual or electronic record, including data stored in emails, documents and notes. This also includes personal data recorded as a result of a phone call or meeting..

As part of their responsibilities staff dealing with personal data must comply with the data protection principles below relating to processing of personal data set out in the GDPR.

(a) Lawfulness, fairness and transparency

(processed lawfully, fairly and in a transparent manner in relation to individuals)

Open Awards make all reasonable efforts to ensure that individuals (data subjects) are aware of the data we hold, for what purpose we hold it, how we use and store it, who we share it with, and how long we hold it for. This is clearly communicated through our Privacy Notice and Privacy Notice for Learners available on the Open Awards website. We require approved Centres to provide learners with clear information about processing their personal data and ensure learners have access to our privacy notice for learners.

All Open Awards forms and documentation requesting personal data carry a personal statement advising of the purpose for collecting the data and link to the privacy notice which provides full details on how we deal with their data. Staff must ensure all new/reviewed forms and documents include these statements.

Open Awards does not knowingly register or collect personally identifiable information from anyone under the age of 13 ("Children"). Staff must adhere to the systems in place to ensure parental/guardian consent has been sought for the sharing of 'children's' data with us before we process their data.

Consent

Should Open Awards need to rely on 'Consent' as the legal basis to process personal data, for example collecting data/images for marketing purposes, formal unambiguous consent must be sought and recorded to capture explicit consent.

(b) Purpose limitation

(collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes)

Staff must ensure that the reason for which we collected the data is the only reason for which it is processed unless the individual is informed of any additional processing before it takes place.

(c) Data minimisation

(adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed)

The personal data we process must be adequate, relevant and not excessive for our legitimate business purposes. Open Awards will not seek to collect any personal data which is not strictly necessary for the purpose for which it is being obtained. Forms and documents for collecting data all carry statements advising of the purpose for collecting the data.

(d) Accuracy

(accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay)

Personal data must be accurate, kept up to date and relevant to the purpose for which we collected it. We must check the accuracy of any personal data at the point of collection and review and update data on a regular basis. The Open Awards procedures on checking accuracy of data should be followed. It is the responsibility of the individual giving their personal data to ensure that this is accurate and Centres should notify us of any changes requiring data to be updated.

(e) Storage limitation

(kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals)

Open Awards undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. The retention periods of personal data is covered by our Data Retention Policy. A data cleanse cycle is in place that all staff must engage in.

Open Awards will dispose of any personal data in a way that protects the rights and privacy of the individual (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

(f) Integrity and confidentiality (security)

(processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures)

All staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised parties. Personal information should be stored on the central database instead of individual spreadsheets/documents where possible. Similarly, data must not be shared though emails or other forms of communication unless there is a legitimate business reason to do so and that data is password protected/encrypted. Particular care should be taken with regard to sensitive personal data and where appropriate this data should always be password protected/encrypted.

Open Awards have in place appropriate security measures that staff must adhere to ensure personal data is secure including a Clean Desk Policy.:

Open Awards will ensure that all personal data is accessible only to those who have a valid reason for using it.
Staff must adhere to our social networking procedures documented in the ICT User Policy and Corporate Branding Guidance and not publish or share personal information processed on any social networking sites.

Open Awards will have in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as 'confidential waste'. Hard drives of PCs and laptops will be wiped clean and disposed of securely. A log will be kept of all disposed equipment and confirmation of data having been removed.

This policy equally applies to staff who process personal data 'off-site', e.g. when working from home.

(g) Accountability

(The controller shall be responsible for, and be able to demonstrate compliance)

Open Awards have appropriate technical and organisational measures in place to ensure that the above data protection principles are implemented and to safeguard individuals rights.

Staff must not disclose personal data without authorisation or agreement from the data subject themselves, the Data Controller, or in line with Open Awards policy. You must maintain data security by protecting the confidentiality, integrity and availability of the personal data:

(a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
(b) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that any authorised users are able to access the personal data when they need it for authorised purposes.

Please note that unauthorised disclosure of personal data may result in disciplinary action.

Record keeping

Full and accurate records of all our data processing activities must be kept. These records should include records of consent forms and procedures for obtaining consent as evidence.

Employee personal data

Personal data provided by employees through the job application and appointment process and ongoing review processes is strictly confidential and will be used securely only for the purposes of employment. Full details of the data we collect, why we collect it, how we store it and how long we keep it for can be found in our Employee Privacy Notice. All staff are responsible for:

- Checking that any information they provide to Open Awards in connection with their employment is accurate and up to date;

- Informing Open Awards of any changes to information which they have provided, eg changes of address;

- Informing Open Awards of any errors in their information. Open Awards cannot be held responsible for any such errors unless the staff member has informed Open Awards of them.

Marketing

You must not collect and store any personal data for marketing purposes unless you have obtained the explicit consent of those individuals. Consent should be obtained at the time when the personal data of the individual is collected. Individuals must be easily able to unsubscribe to any marketing communications. Relevant databases/mailing lists must be kept up to date with details of individuals opting out of receiving marketing communications to ensure we only communicate with people we have received consent from.

Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any personal data breach to the applicable regulator and, in certain instances, the Data Subjects.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Information Systems Officer or Director of Corporate Services.

Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined

Subject Access Rights

Individuals have a right to access any personal data relating to them which are held by Open Awards. This is formally known as a Subject Access Request (SAR). Although Open Awards have a SAR form and process for any individual wishing to exercise this right, a SAR may be submitted in a variety of manner, e.g. a written

request, within the body of any other written communication, email or phone call. Individuals asking for information are not obliged in law to refer to their request as a 'Subject Access Request'; it is therefore essential that staff are able to recognise a request when it is made, whether formally or informally.

You must immediately forward any Subject Access Request you receive to the Information Systems Officer as we are required to respond within a limited time-frame.

We must also verify the identity of an individual requesting data before releasing any information. Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.

Open Awards aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the GDPR guidelines of 30 days.

Procedures for Handling of Personal Data

Open Awards will take the following practical steps to ensure compliance with the Principles of data protection:

1. Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;

2. Meet its legal obligations to specify the purposes for which information is used, by displaying relevant statements on appropriate documentation, and complying with the requirement to notify the Data Protection Commissioner of the purposes of Open Awards processing;

3. Ensure the quality of information used, ie accurate and up to date;

4. Determine and regularly review the length of time information is held, and document this within the Data Retention Policy;

5. Ensure that the rights of people about whom the information is held can be fully exercised under the Act. These include the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information;

6. Take appropriate technical and organisational security measures to prevent the unauthorised or unlawful processing, or disclosure, of data;

7. Ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

8. Ensure that everyone managing and handling personal information is appropriately trained to do so;

9. Ensure that requests from data subjects about access to their personal data are promptly and courteously dealt with;

10. The way personal information is managed will be regularly reviewed and assessed.

Review

This policy will be reviewed in May 2020 or earlier if updates are required to reflect any amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.
Further guidance relating to GDPR is available on the ICO's website www.ico.gov.uk.

Conclusion

Compliance with the General Data Protection Regulation 2018 is the responsibility of all members of Open Awards staff. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken.

Related Policies

Clean Desk Policy
Privacy Notices – Learners, Employees, General/Website
Data Retention Policy
ICT Users Policy
Branding Guidelines (including Social Media)

Definitions

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Data Protection by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR. (this is about considering data protection and privacy issues upfront in everything we do).

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.

Privacy Officer: Information Systems Officer or whoever may be appointed from time to time with responsibility for data protection compliance.

Processing or Process: any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Company's policies, operating procedures or processes related to this Policy and designed to protect Personal Data;

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental

health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.