Data Protection Policy

Stakeholder arrangements for data protection, incorporating the General Data Protection Regulation 25.05.18

Approved by: Board of Directors
Version No. 1 Author: Shaun McNamara
Date Issued: May 2018

Introduction

MJA is responsible for the process of personal data regarding staff, learners and employers relevant to its day to day operations and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, handling, disclosing, transporting and destroying or otherwise using data whether on paper, electronic or recorded on other material. In this Policy any reference to staff, learners or employers includes current past or prospective staff, learners or employers.

Scope

The Policy covers the company's acquisition, handling and disposal of all personal and sensitive data it holds on all staff, learners and employers. It also applies to sub-contracting provision. The policy explains the general approach to data protection which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that **MJA** complies with the Data Protection Act 1998 (the Act) and anticipates the General Data Protection Regulations 2018 (GDPR) which become law on the 25th May 2018.

Definitions

Personal Data is:

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data is:

Any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings. The GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

MJA has additional obligations in connection with the use of sensitive personal data, namely at least one

of the following conditions must be satisfied:

- Explicit consent of the data subject must be obtained.
- Necessary for carrying out the obligations under training, employment, social security or social protection law or a collective agreement
- Used in connection with alumni relations provided it relates solely to this and there is no disclosure to a third party without consent
- Data manifestly made public by the data subject
- Various public interest situations as outlined in the General Data Protection Regulations 2018

The Data Subject:

The person the information relates to, there may be more than one data subject, such as when a record concerns an incident involving two people.

Data Controller:
The person who (either alone or jointly or in common with others persons) determines the purpose for which and the manner in which any personal data is to be processed.

The Data Protection Officer (DPO)
The person whose role within the company is to ensure MJA is correctly protecting individual personal data according to current legislation. MJA has appointed the company's Data and Compliance Officer, currently, Anthony Edwards, who will be responsible for the day to day compliance with this policy.

Obtaining, using and the disposal of personal data
MJA will only process personal data for specific and legitimate purposes, which are as follows:
• For the recruitment, enrolment, education and employment opportunities for current staff and learners and for the future growth of the business
• For personnel, administrative and management purposes, such as staff performance, pay and HR processes
• Communicating with former staff and learners for the purpose of career references and IAG.
• Safeguarding and promoting the welfare of staff and learners and the monitoring of email communications, internet and telephone use to ensure learners and staff are following the company's IT Acceptable Use Policy and all other relevant MJA policies with reference to data protection
• Providing staff, learners and employers with a safe and secure environment, this includes the use of IP cameras in learning suites and reception. Appropriate signs displayed which include appropriate warning signs as to their operation. IP cameras are used for the purpose of detecting crime, ensuring personal security and the welfare of staff, learners, employers and clients/visitors within the centre, footage is stored on a secured server for 24 hours then deleted, but maybe kept for longer in certain circumstances such as an on-going investigation.
• Protecting and promoting the interests and objectives of MJA, by fulfilling the company's contractual and other legal obligations.

Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer's permission.

MJA will not hold unnecessary personal data, but will hold sufficient information for the purpose for which it is required. MJA will record information accurately and will take reasonable steps to keep it up-to-date.

This includes an individual's contact and medical details.

MJA will not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a contact living outside the EEA.

When MJA acquires personal information that will be kept as personal data, MJA will be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

MJA will only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in MJA Retention and Disposal Policy. Permission from the Data Protection Officer for the deletion of records containing personal information must be granted.

MJA will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data. **MJA** uses an internal server that is accessed by authorised staff. Each individual has a login with a secure password; this password is unique and only known to that person. Checks are conducted to ensure passwords are not stored electronically to help prevent unauthorised access.

Storage location of information and security

Information security is the most important aspect of data protection compliance and most of the fines under the Act for non-compliance relate to security breaches. **MJA** will do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the company will take appropriate steps to prevent these events happening.

MJA have a number of manual systems that are used daily for purpose of day-to-day processes, this information is not left unattended by the individual and is securely stored in a lockable facility at the end of the working day or earlier. Client access is restricted in areas that manual data is used.

MJA use a number of systems to retain personal data, an internal server stores staff, learner and employer information for the purpose of conducting day-to-day business activities including processes for recruitment, education, training and/or employment services to all clients connected to **MJA**. The internal server is backed up daily and the potable hard drive (data backup) is taken off site and replaced daily.

MJA uses Eportfolio learning software (Learning Assistant) which provides client and programme information for tracking of learner progress and assesses learner competence whilst working towards a qualification.

Learning Assistant is the central hub, which shares data across to individual accounts. Further information can be found by accessing the following link:
https://www.cityandguilds.com/help/privacy-statement

MJA also uses a web based management software (WEBYETI), which provides client, programme and financial information that is required for the delivery and monitoring of traineeship and apprenticeship programmes contracted by the ESFA (Education Skills Funding Agency). Further information can be found by accessing the following link:
https://www.cognisoft.co.uk/about_cognisoft/privacy/

MJA uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems. Staff are not allowed to remove personal data from the company premises unless it is stored on an encrypted form on a password protected computer, laptop, IPad or memory device.

Staff are trained and know not to use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: including the risk whilst out of the office on business where the risk of theft is greatly increased.

Information and explanation

Privacy Notice:

Purpose:

• privacy notice is to ensure that **MJA**'s collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with, how long records will be retained for and outline the data subject's rights, including the right to complain about the processing of their data to the Data Protection Officer

• MJA are not expected to routinely provide staff, learners and employers with a privacy notice as this should have already been provided. Copy of the company's privacy notice for staff, learners and employers can be obtained from the company website

Use:

• Staff should inform the Data Protection Officer if they suspect personal data is being used in a way which might not be covered by an existing privacy notice. This may be the case where, for example, staff are aware that the company's is collecting medical information about learners without the individual being informed about what the information will be used for.

Protecting Confidentiality internally and externally

Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the company or their relationship to the data subject, unless they need to know it for a legitimate purpose. Examples include:

• Personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to other staff, learners or employers unless the member of staff has given their permission

• Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way

Before sharing personal data outside the company, particularly in response to telephone requests for personal data the following steps are taken:

• Adequate security is in place, meaning it will depend on the nature of the data, for example, if the company is sending starts and leaver's information to the local authority, then the information must be encrypted.

• Sharing information is covered in MJA privacy notice.

Care is taken when using photographs, videos or other personal circumstances such as the case of testimonials and case studies or celebratory news items. Appropriate consent is attained and recorded in accordance with GDPR requirements.

Definitions

Data Breach: A breach of security which can lead to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

Reporting Obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as MJA becomes aware of a significant data breach as determined by the Data Protection Officer it has 24 hours in which to report the breach to the Board of Directors and if necessary the Information Commissioner's Office. Examples of breaches and their seriousness for reporting purposes are:

• Mistakenly sending an email or letter containing personal data to an unintended recipient

• Theft of IT equipment containing personal data

• Failing to deal with a Subject Access Request

If a breach is found to be sufficiently serious i.e. if not dealt with it is likely to result in a high risk to the rights and freedoms of individuals e.g. resulting in discrimination, damage to reputation, financial loss, through identity theft or otherwise, loss of confidentiality or any other significant economic or social disadvantage then not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must also be notified of the breach in a timely manner as directed by the Data Protection Officer.

Data subject's rights and access

Individuals are entitled to know whether MJA is holding any personal data which relates to them, what that information is, and the source of the information. They have the right to know how MJA uses it and who it has been disclosed to. This is known as a Subject Access Request.

Any member of staff, learner and/or client wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer.

Any member of staff who receives a request for information covered by this policy from a learner, employer or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timescale which MJA must follow. Information must be provided to the requestor without delay and at the latest within one month of receipt.

Individuals have the right to:

• Ask MJA not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress

• Ask for incorrect personal data to be corrected or annotated

• Individuals have the right to object to any of their personal data being processed and to have this data erased (except in the circumstances of ESFA and DfE), further information can be found by accessing the link in appendix 1

• Restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected

• Request their personal data is transferred to another data controller in a commonly used format

• Ask MJA not to make automatic decisions (using personal data) if such automatic decisions would affect them to a significant degree.

• To complain about the processing of your personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

Data processors

MJA uses data processors (third parties / organisations) that process, deals with or stores staff, learner and client personal data on MJA's behalf, each third party have written contracts with MJA which include specific terms and reference to data protection as required by the GDPR. Their details can be found in appendix 1

Further information

MJA has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in MJA's register entry on the Information Commissioner's website at https://ico.org.uk/ under the registration number Z607343X. This website also contains further information about data protection.

Breach of the policy

A member of staff who deliberately or recklessly discloses personal data held by MJA without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

Policy Review and Maintenance

This policy will be reviewed annually or as appropriate and in response to changes to legislation or MJA policies, technology, increased risks and new vulnerabilities or in response to security incidents.

Approved by: Board of Directors
Version No. 1 Author: Shaun McNamara
Date Issued: May 2018

Appendix 1

Related Policies:

Staff I.T. Systems & Internet Acceptable Use Policy

Student I.T. Systems & Internet Acceptable Use Policy

Document Retention policy

Data Management & Reporting policy

Safeguarding

Management Information Policy

Social Networking policy

Related Websites – Privacy Notices:

ESFA (Education Skills Funding Agency)

https://www.gov.uk/government/publications/esfa-privacy-notice/education-and-skills-funding-agencyprivacy-notice-may-2018

LRS (Learner Record Service)

https://www.gov.uk/government/publications/lrs-privacy-notices/lrs-privacy-notice

City & Guilds (Awarding Body)

https://www.cityandguilds.com/help/privacy-statement

VTCT (Awarding Body)

https://www.vtct.org.uk/privacy-policy/

ACE

https://acecerts.co.uk/web/privacy-policy

Approved by: Board of Directors
Version No. 1 Author: Shaun McNamara
Date Issued: May 2018