Personal Data Handling Policy - Emerald Tutors

Introduction

Tutors and other staff should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the company to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the company into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office for the company and the individuals involved.

Particularly, all transfer of data is subject to the risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Policy Statements

- The company will hold the minimum personal data necessary to enable it to perform its function, and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the ‘Privacy Notice’ and lawfully processed in accordance with the ‘Conditions for Processing’.

Privacy Notice

Our Privacy Notice can be found here:

http://www.emeraldtutors.co.uk/privacy.html

Conditions for Processing

The conditions for processing are set out in the Data Protection Act. At least one of the following conditions must be met whenever you process personal data:

- The individual to whom the personal data relates has consented to the processing.
- The processing is necessary:
    - in relation to a contract which the individual has entered into; or
    - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you.
- The processing is necessary to protect the individual’s “vital interests”. This condition only applies in cases of life or death, such as where an individual’s medical history is disclosed to a hospital’s A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

- The processing is in accordance with the “legitimate interests” condition.

Personal Data

The company and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or their circumstances. This will include:

- Personal information about members of the company – including pupils, members of staff and parents/carers, e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

Responsibilities

The company’s Data Controller will keep up to date with current legislation and guidance and will determine and take responsibility for the company’s information risk policy and risk assessment

All directors will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to protected data and why

Everyone in the company has the responsibility of handling protected or sensitive data in a safe and secure manner.

Registration

Melisa Jefferies is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – The Privacy Notice

In order to comply with the fair processing requirements of the DPA, the company will inform parents/carers of all pupils of the data they collect, process and hold on the pupils, the purposes for which the data is held and the third parties, if any, to whom it may be passed. This privacy notice will be passed to parents/carers when their child enrols in a course.

Training and Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy, through:

- Induction training for new staff
- Staff Meetings/Professional Development Sessions
- Day-to-day support and guidance

Risk Assessments

Information risk assessments will be carried out by the Data Controller to establish the security measures already in place and whether they are the most appropriate and cost-effective. The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form:

Risk ID	Information Affected	Protective Marking (Impact Level)	Likelihood	Overall Risk	Actions to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government published HMG Security Policy Framework [http://www.cabinetoffice.gov.uk/spf], which recommends that the Government Protective Marking Scheme is used to indicate the sensitivity of data. The scheme is made up of five markings, which are mapped to Impact Levels as follows:

Label	Usage	Impact Level (IL)
UNCLASSIFIED		0
PROTECT		1
RESTRICTED		2
CONFIDENTIAL		3
HIGHLY CONFIDENTIAL		4
TOP SECRET		5

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, e.g. the home address of a child (or vulnerable adult) at risk, will be marked as RESTRICT.

The company will ensure that all staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to and the handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered ‘unclassified’. The term ‘UNCLASSIFIED’ may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated, the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. 'Securely delete or shred this information when you have finished using it'.

Password Security Policy

- User passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected and must be locked if left (even for very short periods).
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

When personal data is stored on any portable computer system, USB stick or any other removable media;

- the data must be encrypted and password protected
- the device must be password protected
- the data must be securely deleted from the device, in line with policy once it has been transferred or its use is complete

All paper-based Protected and Restricted (or higher) material is held in lockable storage

The company recognises that data subjects have a number of rights in connection with their personal data, the main one being the right of access.

Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them.

Under certain circumstances, the data subject can also exercise rights in connection with the rectification, blocking, erasure and destruction of data. Parents/Carers may request to see a copy of the information held about them and their children. Requests are made to the data controller. This right to request is clearly indicated in the Privacy Notice on the website.

Secure transfer of data and access out of the company

The company recognises that personal data may be accessed by users outside of company premises, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted, or protected personal data from the company or authorised premises without permission, and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members)
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should have secure remote access to the management information system. If secure remote access is not possible, users must only remove or copy personal or sensitive data from the

organisation or authorised premises if the storage media, portable or mobile device, is encrypted and is transported securely for storage in a secure location

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (NB. The carrying of encrypted material is illegal in some countries)

Disposal of Data

The company will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded or otherwise disintegrated for data.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	**The technology**	**Notes on Protect Markings (Impact Level)**
Learning and achievement	Individual academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically, information will be exchanged with parents through email.	PROTECT (Impact Level 2)
Messages and alerts	Attendance, behavioural, achievement, sickness, and other information that may be important to inform or contact a parent about as soon as possible.	Email and text messaging are commonly used to contact and keep parents informed.	PROTECT (Impact Level 1) However, it is not practical to encrypt email or text messages to parents, schools so detailed, personal information will not be sent by these methods

Privacy Notice

Emerald Tutors is a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your child's school. We hold this personal data and use it to:

- Support its pupils' teaching and learning;
- Monitor and report on their progress;
- Provide appropriate pastoral care
- Assess how well the company is performing in its educational tasks.

This information includes contact details, previous education information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about you to anyone outside the company without your consent unless the law requires it.

We may be required by law to pass some information about you to the Local Authority and the Department for Education (DfE) and to agencies that are prescribed by law, such as the Qualifications and Curriculum Authority (QCA), Ofsted, the Learning Skills Council (LSC), the Department of Health (DH) and Primary Care Trusts (PCT). All these are data controllers in respect of the data they receive and are subject to the same legal constraints in how they deal with the data.

If you want to see a copy of the information about you that we hold and/or share, please contact The Data Controller at info@emeraldtutors.co.uk