

**Policy Name:Data Protection Policy**

|  |  |  |  |
| --- | --- | --- | --- |
| Date policy written/amended | Amended/written by | Authorised by | Next review due |
| 22.8.2016 | Sarah cox | Sarah cox | August 2017 |
| 30/8/18 | Sarah Cox | Sarah Cox | August 2019 |
|  |  |  |  |
|  |  |  |  |

**1**

**Data Protection Policy**

1.1 The board of directors of the Melton Learning Hub, as the body corporate with responsibility for managing the charity, is the designated data controller responsibility for data protection under the Data Protection Act 1998. The board delegates specific responsibilities to the Manager for ensuring that the policy is adhered to and updated as necessary, but remains data controller with overall responsibility under the Act.

1.2 The Manager is the named person at The Hub with responsibility for personal data and any staff queries should be addressed to them.

1.3 The board of Directors has a responsibility to notify the Information Commissioner’s Office (ICO) that it is processing personal data and will be given a registration number. The ICO needs to be informed of serious breaches of data protection.

1.4 The Board of Directors will prepare a privacy notice, that sets out what personal information it collects and why. This privacy notice will be published on the Melton Learning Hubs website

**Personal data –Privacy Notice**

2.1 The charity holds personal data about students and staff.

2.2 In the case of students we collect personal information from parents and previous schools and the Learning Record Service. We hold this personal data to:

 \_Support student learning;

 \_Monitor and report student progress;

 \_Provide appropriate pastoral care, and

 \_Assess how well we are doing.

Information about students that we hold includes contact details, national curriculum assessment results, attendance information and personal characteristics such as ethnic group, any special educational needs and relevant medical information.

2.3 Personal data and school records about students are confidential to the child. The information can be shared appropriately within the professional working of the hub to enable the school or the trust to make the best educational provision for the child. The law permits such information to be shared with the Department for Education, Local authorities and other educational establishments when students change schools.

2.4 the Hub should have a clear procedure for ensuring that student records are kept up to date.

2.5 In the case of employees we collect personal information to assist in the smooth running of the Hub and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

• Improving the management of Hub workforce data across the sector;

• Enabling a comprehensive picture of the workforce and how it is deployed to be built up;

• Informing the development of recruitment and retention policies;

• Allowing better financial modeling and planning;

• Enabling ethnicity and disability monitoring; and

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

2.6 We will not give information about staff to anyone outside the Hub without their consent unless the law and our rules allow us to. We are required by law to pass on some of this data to the Local Authority and the Department for Education.

2.7 Employees have consented in their employment contract to the data being used as set out in the contract. If this data changes, they should let the trust know so that our records can be updated.

**Protection principles**

3.1 The data protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These are that personal data must:

 \_be fairly and lawfully processed;

 \_be processed for limited purposes and not in any manner incompatible with those purposes;

 \_be adequate, relevant and not excessive;

 \_be accurate;

 \_not be kept for longer than is necessary;

 \_be processed in accordance with individuals' rights;

 \_be secure; and

 \_not be transferred to countries without adequate protection.

**Information security measures**

***Paper security***

4.1 All paper held personal data should be stored in secure and locked cabinets in rooms that are locked and alarmed when not in use. The physical security of premises should be checked regularly.

4.2 Employees who take home appropriate paper copies of personal data to support their work should ensure that the data is protected at all times. Files should be cared in closed bags and securely locked in the boots of cars, and employees should not work on files in public spaces including trains.

4.3 Waste paper containing personal data should be shredded.

***Email and fax security***

4.4 Transmit information between locations only if a secure network or comparable arrangements are in place or if, in the case of email, encryption is used.

4.5 Pay particular attention to the risks of transmitting confidential information by email or fax including:

 \_The use of the auto-complete email address function and group email addresses.

 \_Failure to inform the recipient that a fax containing confidential data is being sent and the failure to use a cover sheet to highlight sensitive information.

4.6 Ensure that all copies of email and fax messages received are held securely and that time expired messages are erased securely.

4.7 Consider whether the use of a courier service would be more appropriate than a fax or an email.

4.8 If a fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine and ring up or email to make sure the whole document has been received safely.

***Computer security***

Ensure computer security by:

 \_Installing a firewall and virus checking on computers and encrypting laptops.

 \_Making sure that operating systems receive regular automatic updates.

 \_Protecting computers by downloading the latest patches or security updates, which cover vulnerabilities.

 \_Only allowing staff access to the information they need to do their job

 \_Using complex passwords, changing them regularly and never sharing them.

 \_Encrypting personal information held electronically that would cause damage or distress if it were lost or stolen.

 \_Taking regular back-ups of information and keeping them in a separate place.

 \_Securely removing all personal information before disposing of old computers.

 \_Installing anti-spyware software on all computers.

**Websites, Newsletters, Newspapers and CCTV**

5.1 Do not disclose personal information (including photos) on a website, in a Hub newsletter or in a newspaper without the individual pupil, member of staff or director being aware. Student photographs should not be published on a website, in a hub newsletter or in a newspaper without parental consent.

5.2 CCTV cameras are installed in the Hub to enhance security and help maintain good order. They should be sited where they are needed for the stated purpose and where they do not unnecessarily intrude on anyone’s privacy.

**Staff training and security**

6.1 All employees should be trained to:

 \_know what is expected of them;

 \_be wary of people who may try to trick them into giving out personal details;

 \_be aware that they can be prosecuted if they deliberately give out personal details without permission;

 \_use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;

 \_never send offensive emails about other people, their private lives or anything else that could bring their organization into disrepute;

 \_highly suspicious of emails that appear to come from their bank that ask for their account, credit card details or your password (a bank would never ask for this information in this way);

 \_not open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

**Access to personal data**

7.1 Under the Data Protection Act students and employees have a right of access to their own personal data held by the trust. In the case of an employee or a parent requesting access to their child’s records, a request for access must be made in writing. All requests will be acknowledged in writing and access to records will be made as soon as possible but no later than 40 days in the case of personal information or 15 school days in the case of educational records.

7.2 For staff and students there is no charge for such requests but there may be a charge for parents if the request for access requires the photocopying of records.

7.3 From the 1st January 2005, when the Freedom of Information Act came into force, a request for personal data can include unstructured as well as structured records eg letters, emails etc. not kept within personal files, or filed by their name, but still directly relevant to them.

**Retention of employee records**

|  |  |
| --- | --- |
| 9.1 In relation to the retention of employee records, the hub follows the retention periods recommended by the Information Commissioner in its Employment Practices data protection Code. Application form | Duration of employment |
| References received | 1 year |
| Payroll and tax information | 6 years |
| Sickness records | 3 years |
| Annual leave records | 2 years |
| Unpaid leave/special leave records | 3 years |
| Annual appraisal/assessment records | 5 years |
| Records relating to promotion, transfer, training, disciplinary matters | 1 year from end of employment |
| References given/information to enable references to be provided | 5 years from reference/end of employment |
| Summary of record of service, eg name, position held, dates of employment | 10 years from end of employment |
| Records relating to accident or injury at work | 12 years |