Apple Blossom Kindergarten

DATA PROTECTION POLICY

Apple Blossom Kindergarten/Manchester Steiner Ltd.

Introduction

Apple Blossom Kindergarten managed by Manchester Steiner Ltd. collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the school in order to provide education and associated functions. In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities, government agencies and other bodies.

This policy is intended to ensure that personal information is dealt with properly, securely and in accordance with the **Data Protection Act 1998** and other related legislation. The policy applies to all personal information, regardless of the way it is used, recorded and stored, whether that be in paper files or electronically.

Data covered under the 1998 Act

- All personal data (facts and opinions)
- Data held electronically and manually
- E-mail

Duties of Manchester Steiner School under the Data Protection Act 1998

- To be a registered user of data within the Data Protection Act
- To comply with subject access requests
- To comply with the eight Data Protection Principles

The Eight Data Protection Principles

These principles, as laid down in the Data Protection Act 1988 and which must be followed at all times, state that data must be;

1. Fairly and lawfully processed
2. Processed for limited, specific and lawful purposes
3. Adequate, relevant and not excessive in relation to purpose
4. Accurate and, where necessary, kept up-to-date
5. Kept no longer than necessary for purpose
6. Processed in accordance with the rights of data subjects under the Act
7. Appropriately held to protect against unauthorised or unlawful processing, or accidental loss, damage and destruction
8. Prevented from being transferred to countries outside the EEA without adequate protection

Applying the Principles in Practice

The school will:

- explain for what purposes information is being collected
- explain why, with whom and under what circumstances information will be shared
- check the quality and accuracy of the information we hold
- ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures to safeguard any personal information
- share information with others only when necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act
- ensure all our staff are aware of the relevant policies and procedures

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Complaints

Complaints under this policy should be made to the Data Protection officer (currently Kate Gray), who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. If the Data Protection officer is unable to resolve a complaint, it will be referred to the Manchester Steiner School Project Committee. Complaints which are not dealt with under the school's complaint procedure should be forwarded in writing to the Information Commissioner.

It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the Data Protection officer. Complaints that involve consideration of personal data or sensitive personal data should be referred to the directors. If the complaint is not successfully resolved by the Manchester Steiner School Project Committee it will be referred to the Information Commissioner.

Contacts

If you have any concerns or questions in relation to this policy please contact the Administrator, who will also act as a contact point for any requests under the Data Protection Act.

For advice and assistance please contact the Data Protection officer (currently Kate Gray).

Further advice and information, including a full list of exemptions, is available from the Information Commission, www.informationcommissioner.gov.uk

Policy by: Kate Gray **Date:** November 2015
Designated director responsible for approving this policy: Kate Gray **Signature:** **Date**: Sunday, 20 November 2016
Reviewed: 20th November 2016
Next Review Date: November 2017

Data Protection: Practical Guidelines for Staff

To ensure that we care adequately for all personal data we will:

- Have a clear desk policy
- Be security conscious
- Configure screensavers with timeouts and passwords
- Change passwords that provide access to any private data regularly
- Not supply information to external agencies over the telephone
- Keep clear records of any information that is supplied to external agencies
- Not retain unnecessary information
- Use and maintain passwords privately and securely

In handling personal data we will:

- Treat the personal data of others as we would expect our own data to be treated
- Be professional and accurate in complying with the Data Protection Principles
- Ensure confidentiality and prevent unlawful disclosures as an absolute necessity
- Insist on information security as a paramount requirement
- Remember that people have a right to privacy, and remember that and respecting this right is expected from all those who handle personal data

What does this mean for us on a daily basis?

- **REMEMBER**: Data protection is about all data and not just data on a computer
- **Clear Desk Policy:** File away **ALL** private data at the end of every day
- **Think about your emails**
    - Who has access to them?
    - Who are they for?
    - Are other peoples email addresses are visible?
        - Do you have the right to share someone's email address
    - What information have you included?
    - Are you forwarding someone else's email?
        - Do you have the right or the need to do this?
- **Think about who you share information with and how**
    - What do they need to know?
    - Do they know how to handle data securely?
    - Do they actually need a separate copy of the information?
    - If you are in conversation with someone – who can over-hear?
    - Who can overhear you when you are on the phone?
- **We are all 'voices of Manchester Steiner School Project'**

Procedures for Responding to Requests for Personal Information in Accordance with the Data Protection Act (1998)

Anybody who asks to see their file, their child's file or other personal data held on them is making a request under the Data Protection Act 1998. All information relating to the child, including that held in day books, diaries and on electronic systems and email should be considered for disclosure.

Parents have an automatic right to access defined materials under The Education (School Records) Regulations 1989 unless save any information considered under section 9 (Savings) of these Regulations. The school will observe these statutory rights.

If there is a current court order which relates to information regarding any child, that order must, regardless of other circumstances, be observed.

Dealing with a Data Protection Request

1. A request under the Data Protection Act must be made in writing.
2. In many cases a letter to the Administrator will be sufficient to identify the information required. If you cannot identify the information required from the initial request you can go back to the applicant to ask for more information.
3. The Administrator must be confident of the identity of the individual making the request. This could be done by checking signatures against verified signatures on file or by asking the applicant to produce valid identification, such as a passport or photo-driving license. These checks should be done in addition to proof of relationship with the child.
4. An individual only has the automatic right to access information about themselves; requests from family members, carers or parents of a minor will have to be considered. The Administrator will have responsibility for ensuring the child's welfare is appropriately considered in deciding whether to comply with a request. Normally the requester will have to prove both their relationship with the child and that disclosure is in the child's best interests to the satisfaction of the Administrator. In the event of a child having sufficient capacity to understand (normally only children in Class 8, as advised by the Class teacher), the Administrator should discuss the request with the child and take their views into account when making a decision. There may be circumstance in which a child can refuse their consent to a request.
5. The school may charge a statutory fee, currently calculated on a sliding scale, but only if a permanent copy of the information is provided. If a letter is sent out requesting a fee the 40-calendar day statutory timescale does not begin until the fee is received. It is important though that no request is delayed unnecessarily by time taken to inform the applicant of a fee.
6. The school will make use of exemptions under the Act as appropriate. All files must be reviewed before any disclosure takes place. Under no circumstance will access be granted immediately or before this review process has taken place.
7. Where information has been provided to the School by a third party, for example by the local authority, the police, a health care professional or another school, but is held on the school's file it is normal to seek the consent of the third party before disclosing information. This must be done early in the process in order to stay within the 40-day timescale. Even if the third party does not consent or consent is explicitly not given the data may be disclosed. In these cases it may be appropriate to seek additional advice.

8. The applicant should be told the data that the school holds, be given a copy of the data, be told the purposes for which it is processed and whether it has been shared with any other party. It is good practice to explain whether data has been withheld and if so why. There may be circumstances where this is not appropriate; the Administrator should at all times consider the welfare of the child. The school should also give details of who to contact in the event of a complaint and the details of the Information Commission who can provide independent information.
9. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or parts of the data can be retyped if this is more sensible. In any event a copy of the full document (before obscuring) and the altered document should be retained together with the reason why the document was altered. This is so, that in the event of a complaint, there is an audit trail of what was done and why.
10. Information can be provided by post (registered mail) or on deposit at the school with a member of staff available to help the applicant. If the latter is used the applicant must have access to a photocopier in case they want a permanent copy of their data. In considering the method of delivery the views of the applicant should be taken into account. Any codes, technical terms or abbreviations should be explained. Any data which is difficult to read or illegible should be retyped.
11. Schools should monitor the number of requests received and document whether they are dealt with within the 40-calendar day statutory timescale.
12. The Act applies only to living individuals.