Writtle Infant School

Lodge Road, Writtle, Chelmsford, Essex, CM1 3HZ

Data Protection Policy

Date of policy:	January 2012
Date last review adopted by governing body:	07/11/2017
Frequency of review:	Three yearly

1. Introduction

Writtle Infant School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Our Data Protection Office is: Essex County Council

2. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR act of 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3. What is personal information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. We hold names, addresses, date of birth, contact details, attainment and progress data, medical and SEND needs data and other personal information that parents need us to hold about the children , for example allergies, personal circumstances etc. We also hold information about the staff, contact details, date of birth, medical and other personal details, absence, pay and qualifications. The information comes from the parents and on occasions from the children, for example when a disclosure is made. We verify ages of individuals with checking of birth certificates and other identification such as passports and driving licenses. It also includes photos and CCTV, files and information held electronically, on central files and correspondence and notes held across the school.

Our Photography in schools policy details our approach to images. Our website can only be accessed by particular staff and we do not use the website for data sharing, there are secure areas for that for staff and governors.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

4. Data protection principles

In accordance with the GDPR act of May 2018:

We hold names, addresses, DOB, contact information of parents and other individuals who are contacts for the children, information about particular children such as parental access, medical and SEND needs. We also hold information about social care referrals and other notes that are relevant and important for the care of the child concerned.

We do not share personal data without the permission of the parents/carers, unless it is a social care referral where we are advised that informing the parents would put the child at risk. However there are also other cases where we can give consent, for example if a parent refused us holding contact data we have to for the safety of the child.

1. The GDPR brings in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. This applies to ages 13 and over
2. The new intake forms will give the parent or guardian's consent to process the data lawfully
3. If personal data is breached, the GDPR insists that the ICO is informed.
4. A Privacy Impact assessment will be a legal requirement and would need to be re-done when there is a high-risk situation such as new technology being employed.
5. There has to be a privacy statement on the front page of the website and sections staff and parents/children
6. There have to be records of processing activity for all data groups on the website
7. All public bodies will appoint a Data Protection Officer who cannot be anyone involved in the data as the DPO holds them to account

8. There must be monthly status updates for all systems
9. All staff will have training on the GDPR which is regularly updated

5. Subject access requests

Data protection legislation entitles an individual the right to request the personal information a school holds on their behalf – this is known as a Subject Access Request and includes all and any information held by the school, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in the school.

SARs must be responded to within 40 calendar days of receipt. The SAR should be made in writing by the individual making the request. The school may charge a fee for dealing with this request, typically £10. Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

6. General statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures
- Child Protection information is kept in a locked metal safe
- Ensure that the rights of individual under the GDPR are respected. These are:
    - Subject access
    - To have inaccuracies corrected
    - Have information erased (note contact details etc. would not be erased until the child has left the school). Also information such as SEND records and Child Protection records would not be erased as per legal requirements. The new act of 2018 gives people a stronger right to have their data deleted, however we will use the legal requirements we have as our legal basis whether to proceed or not. The legal basis for processing the data would need to be explained. If there is a complaint the data must be temporary suppressed
    - Prevent direct marketing
    - Prevent automated decision making and profiling
    - Appropriate data portability – any data that is shared is done via the expected procedures, e.g. common transfer for new and leaving pupils

- If information is used for any profiling, for example prediction SAT results, this must be made explicit
- If data is breached there must be clear agreement between the data controller and the school as to how it is addressed and how personal information is securely processed

7. Security

Data Controllers should ensure that data is physically secure (e.g. lockable cupboards) and access to information held in hard copy is only accessible by those with a need to use it to do their job.

IT systems that back-up personal information should also be reviewed to ensure that these arrangements are also effective. Portable devices (e.g. laptops, memory sticks) that hold personal information are password protected. If hard copies of data need to be taken from their secure home the Headteacher and Data Protection officer must be aware of this.

Any failure to use adequate software to safeguard personal information will invoke action from the ICO.

All staff are aware of how data is disposed of.

Hard copy data is shredded; soft-copy data is cleared from the files and memory of devices and IT support colleagues should confirm that records have been cleared.

When sharing files with other organisations such as local authorities, other schools and social services we ensure that we have the consent to share information (for example on new-entrant forms and agreements signed by parent/carers that come with information requests from social care) and security arrangements are in place to protect the information. For example social care information is sent via a protected password and using a secure e-mail. Sensitive information is delivered by hand.

8. Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

9. Equality statement

"The governors and staff are committed to providing the full range of opportunities for all pupils regardless of gender, disability, and ethnicity, social, cultural or religious background. All pupils have access to the curriculum and the right to a learning environment which dispels ignorance, prejudice or stereotyping."

10. Our school values

Following input from all stakeholders, the school has decided on these five core values which underpin everything we do as a school.

- Honesty
- Independence
- Politeness

- Inclusivity
- Perseverance

11. Role of Governors

Governors determine, support, monitor and review the school policies.

12. Contacts

If you have any enquires in relation to this policy, please contact the Headteacher who will also act as the contact point for any subject access requests. Further advice and information is available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 123 1113. We register with the ICO every year.

APPENDIX 1

Writtle Infant School procedures for responding to subject access requests made under the General Data Protection Regulations of 2018

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.
1. Under GDPR regulations of 2018, any individual has the right to make a request to access the personal information held about them.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher**.** If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (age 13 or above) and the nature of the request.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought. From 2018 it will be one month. In addition we will need to provide additional information such as data retention periods and the right to have inaccurate data corrected.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures then please contact the Headteacher. Further advice and information can be obtained from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 123 1113.