

Arkholme Church of England Primary School



Data Protection Policy 2017-2019

Arkholme C of E Primary School

Data Protection Policy

Arkholme CE Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Arkholme CE Primary School needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are stated according to GDPR.

In summary these principles state that personal data shall:

- (a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this

Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

Fair Obtaining

The School undertakes to obtain and process personal data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' rights of access. Information about the use of personal data is printed on the appropriate collection form, if details are given verbally the person collecting will explain the issues before obtaining the information.

The Data Controller and the Designated Data Controllers

The School, as a body, is the Data Controller under GDPR, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has identified its Designated Data Controllers as:

The Head teacher and the School Clerk.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Head Teacher, in the first instance.

Responsibilities of Staff

All staff are responsible for:

1. Checking that any information that they provide to the School in connection with their employment is accurate and up to date.
2. Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.
3. Handling all personal data (eg – pupil attainment data) with reference to this policy.
4. The School Clerk will issue parents with a copy of the Data Protection Statement upon registration of their child at Arkholme.
5. At the beginning of each academic year the school Clerk will issue parents a copy of the information held in respect of their child and request details of any changes to personal details which may be required.

Data Integrity

The School undertakes to ensure data integrity by the following methods:

Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances their record will be updated as soon as is practicable. Where a data subject challenges the accuracy of their data, the School will try to resolve the issue informally but if this is not possible, any disputes will be referred to the Board of Governors for their deliberation.

In order to prevent such problems we shall provide data subjects with opportunities to check their data accuracy and request amendments.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive to the purpose for which the data is held. In order to ensure compliance with this principle, the School staff will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the School staff, with appropriate guidance, to ensure obsolete data are properly erased.

Data Security

All staff are responsible for ensuring that:

1. Any personal data that they hold is kept securely (see definition below regarding what constitutes secure storage).
2. Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information will be:

- Be kept in a filing cabinet, drawer, or safe in a secure office, or;

- If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a USB drive or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.

Authorised Disclosures

In general, the School will only disclose data about individuals with their consent. However, there are circumstances under which the school's authorised officer(s) may wish to reveal data without express consent.

These circumstances are intentionally limited to :

- Pupil data disclosed to authorised recipients in respect of education and administration necessary for the school to perform its legitimate duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their children's health, safety and welfare.
- Pupil data disclosed to parents in respect of their children's progress, attendance, attitude and general demeanour within and in the vicinity of, the school.
- Staff data disclosed to the relevant authority in respect of payroll and schools' staff HR administration
- Other disclosures as may prove unavoidable, for example where an incidental disclosure occurs when an IT engineer is servicing the school's computer systems. In such cases, the IT engineers under contract to the school will have signed a confidentiality agreement and will not disclose such data outside the school. Education Authority IT Liaison/Support Officers are professionally bound not to disclose such data.
- Only authorised officers are allowed to make external disclosures of personal data. Data used within the school by the school clerk, teachers and welfare workers must be made available only if the staff member needs to know the information for their work within the school.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under GDPR.

The School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users has a right under GDPR to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Head teacher. The School will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.

The School may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by GDPR.

Retention of Data

The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

Transfer of records and data

Confidential records are shared where there have been child protection concerns according to the process required by our Local Safeguarding Children Board.

The procedure guides this process and determines what information we can and cannot share with a receiving school or setting.

Procedures

The procedures for the transfer of records for a child moving to another early years setting or school are as follows:

- Contact is made with the new / receiving school and an official start date is obtained.
- The new school's DCSF number is verified in order to forward a CTF (electronic record of Sims data) via secure S2S system. The CTF will include attendance, SEN and SAT's data relevant to the pupil.
- A hard copy of end of year reports, previous admission templates and copies of important medical information is collated to be sent by recorded delivery to the receiving school.
- Further information including any additional needs that have been identified or addressed by the school, any special needs or disability, whether a CAF was raised in respect of special needs or disability, whether there is a Statement of Special

Educational Needs, and the name of the lead professional will also be sent to the receiving school via recorded delivery.

- If there has been any welfare or protection concerns, this information will be transferred securely to the new school.

Transfer of confidential information

The receiving school or setting will need to have a record of any safeguarding or child protection concerns that were raised at Arkholme and how these were addressed. A summary of the concerns will be made to send to the receiving setting or school, along with the date of the last professional meeting or case conference.

Where a CAF has been raised in respect of any welfare concerns the name and contact details of the lead professional will be passed on to the receiving setting or school.

Where there has been a s47 investigation regarding a child protection concern the name and contact details of the child's social worker will be passed on to the receiving setting or school – regardless of the outcome of the investigation.

This information is posted via recorded delivery or taken to the school or setting, addressed to the setting or school's designated person for child protection and marked as 'confidential'.

Monitoring and Evaluation

This is ongoing; where any clarifications or actions are needed the Policy will be amended at its next review.

Date:	<i>Jan 2017</i>
Review period:	<i>Two years</i>
Reviewing body:	<i>Resources subcommittee</i>

Subject Access Request Form

Section 1

This form is used by Arkholme C.E. Primary School to help you to receive information we hold and process about you, the data subject (the term used for the person whose information is held by the school).

Please complete the form as fully as possible - if you do not it could make it difficult for us to process your request.

If you are applying on behalf of another person, with their consent, please include proof of your right to do so. If you need help completing this form please contact the school office.

Data subject's name _____

Address _____

_____ Post code _____

Previous address if you have moved since your details were given to the school

_____ Post code _____

Section 2 (Please tick)

Are you the data subject named above?	Yes	No	If yes please proceed to section 4
Are you the parent/guardian of the child pursuing your separate right to access your child's official educational records?	Yes	No	If yes please proceed to section 4
Are you the parent/guardian of the child and acting on behalf of a child does not understand the nature of their own access rights?	Yes	No	If yes please proceed to section3
Are you acting on behalf of the person named above?	Yes	No	If yes please proceed to section3

Section 3 If you are acting on behalf of the data subject

Do you have written permission	Yes	No	If yes please attach a copy and proceed to section 3a
--------------------------------	-----	----	---

Section 3a Please complete the following declaration

I (Applicant) declare that **I am an agent** acting on behalf (the data subject) with their full knowledge and written consent(enclosed), or on behalf of a child who does not understand the nature of the request and I am acting in their interest. I will only disclose the information to the data subject except with further authorisation from them.

SignedAgent / Parent.....

Section 3b Details about the agent

Data subjects name _____

Address _____

_____ Post code _____ Tel _____

Section 4

Please state in your own words what information you require, include details of any reference numbers given to you like payroll or client numbers, or reasons why you believe the school has your personal information in its files.

Section 5 Declaration

To be signed by all applicants I declare that the information given in this form is correct and that I am the data subject, parent or agent.

Signed..... Date.....

The school has 15 school days to respond to a request for educational records and 40 calendar days to respond to other requests. The information you provide on this form will be used only for the purposes of processing your request.