Newbottle and Charlton
C.E.V.A. Primary School
Every Person Matters, Every Moment Counts
'I can do all this through him that gives me strength'

Charlton
Banbury
Oxon
OX17 3DN

Telephone/Fax:
(01295) 811480

Email: bursar@newbottle.northants-ecl.gov.uk

Head Teacher:
Mr Peter Smith

Chair of Governors:
Lady Deborah Hayter

DATA PROTECTION POLICY & FREEDOM OF INFORMATION PUBLICATION SCHEME

(Statutory – Biennial Review)

Reviewed & adopted by the Full Governing Body	10 July 2023
Chair of Governors Signature:	
Date of next review:	June 2025
Related Policies:	E-safety Policy Pupil & Parent Privacy Notice Staff Privacy Notice
Data Protection Officer (DPO)	Judicium Education

Data Protection Policy and Freedom of Information Publication Scheme

Purpose
Newbottle & Charlton CEVA Primary 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. The school aims to comply with the Retention Guidelines laid down by statute.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with all relevant Data Protection Legislation (collectively referred to as Data Protection Legislation/General Data Protection Regulation (GDPR)).

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by reading and adhering to these guidelines. Staff will also be trained on an annual basis to ensure their understanding.

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.

Data Protection Principles
Data Protection Legislation requires that personal data shall be:

1. Processed fairly and lawfully and in a transparent manner in relation to individuals;
2. Obtained only for one or more specified and lawful purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purposes for which the personal data are processed;
6. 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 and organisational measures.

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

- Inform individuals why the personal information is being collected and who it is being shared with when it is collected
- 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, it is done so appropriately and securely
- Ensure that 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 appropriate to do so under the specified and lawful purposes. Steps will be taken to ensure data is shared with third parties that comply with Data Protection Legislation.
- Keep a record of any third parties which we share data with as part of our privacy notices
- 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

Data Breaches
The Data Protection Legislation places a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. Data breaches must be reported where it is likely to result in a risk to the rights and freedoms of individuals and must be reported to the ICT a maximum of 72 hours from when the breach is identified. The school will detect, report and investigate personal data breaches.

Data Protection Officer (DPO)
We have an appointed DPO. The tasks of the DPO include as a minimum:
- To inform and advise the school and its staff about their obligations to comply with Data Protection Legislation
- To monitor compliance with Data Protection Legislation, including managing internal data protection activities, advising on data protection impact assessments; training staff and conducting internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (pupils, employees etc)
- To manage subject access requests and data breaches with both staff and external organisations

Freedom of Information Publication Scheme
Procedures for responding to subject access requests made under the Data Protection Act 1998 and subsequent legislation.

Rights of access to information
There are two distinct rights of access to information held by schools about pupils.
1. Any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Educational regulations.

These procedures relate to subject access requests made under the Data Protection Act 1998 and GDPR legislation.

Actioning a subject access request
1. Requests for information can be received by any staff member and it does not need to state it is a SAR. 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 (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school will not charge for an initial SAR. Should multiple requests be made for the same information then a charge may be imposed by the school to cover reasonable administrative work.

5. The response time for an SAR is 1 calendar month. The effective start date will commence when the school receives the request. If the SAR is complex in nature the school may extend its response time to three (3) months.

6. The Data Protection Legislation allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure.

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 response times outlined above.

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. The Data Protection Office is responsible for authorising redaction of any data. This will only be authorised after advice from the Information Commissioner's Office has been 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.

13. Requests that are manifestly unfounded or excessive, including repetitive requests, may be refused. In this situation an explanation will be provided including information on the right to complain to the supervisory authority as outlined below.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints which are not appropriate to be dealt with through the school's complaint procedure can be

dealt with by the Information Commissioner's Office (ICO). Contact details of both will be provided with the disclosure information.

Review
This policy will be reviewed every 2 years. The policy review will be undertaken by the school's Resources Committee.

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

References
Policy developed using guidance from Information Commissioner Office www.ico.gov.uk