BIRCH COPSE PRIMARY SCHOOL
DATA PROTECTION POLICY

Document Control	
Version	3.0
Date approved:	May 2026
Reviewed by	Paul Massey (Acting Head)
Approved by	Governing Board
Next review date	May 2027
Review Frequency	Annually
Status (statutory/ non-statutory)	Statutory

Version History		
Version	**Date**	**Notes/ changes**
1.0	2019	Policy implemented: 15th May 2019
1.1	2023	
2.1	05/2025	Rewrite based on best practice guidance from West Berkshire
3.0	05/2026	Rewrite using Model WB Policy

This policy is adapted from a West Berkshire Council model policy and guide for schools

Aims & Objectives:

The aim of this policy is to provide a set of guidelines to enable all members of Birch Copse School community to understand:

- The law regarding personal data
- The importance of Personal Data governance
- How personal data should be processed, stored, archived and deleted/destroyed
- How staff, parents and pupils can access personal data
- Examples of good practices

The objective of the policy is to ensure that Birch Copse School acts within the requirements of the Data Protection Act 2018 and General Data Protection Regulation (UK-GDPR) when retaining and storing personal data, and when making it available to individuals.

Data Protection – the law:

- Under the Data Protection Act 2018, and other regulating Acts, access to their own personal data is a statutory right for pupils (if they are of an age to understand the data they request) and parents (as defined in the Education Act 1996) may also request access to their child's personal data.
- All members of the community have a right of access to personal data controlled by the school on the individuals.
- Anyone has the right to question and correct inaccurate data, but this must be matters of fact, not opinions.
- Personal data should always be kept securely and protected by passwords if it is electronic, and processing of the data should only be by those authorised to do so – maintaining privacy is the school's responsibility.
- The law also provides that personal data should not be kept longer than is required.
- Third party data (information about someone other than the requesting individual) should in general only be provided with their permission.
- Birch Copse School has appointed a Data Protection Officer (DPO) to oversee compliance with data protection requirements. The DPO is Gerard Strong (West Berkshire Council), who can be contacted at gerard.strong1@westberks.gov.uk
- The School Business Manager retains day-to-day responsibility for data protection within the school. All queries relating to data protection should be directed to the DPO in the first instance.

The importance of Personal Data governance:

The smooth running of a school involves a high level of trust amongst all members of the school community. When large amounts of personal data are being stored in IT and paper-based systems set up by the school, data protection is an important responsibility for all members of staff.

There are many benefits: - imagine the time we can all save from sharing a well organised archive where teachers can search for pupil data easily; imagine the reputational damage the school would suffer from when

ransomware managed to get onto our school system and we have to pay a large sum of money or suffer from days of system outage?

Fair processing of personal data: data which may be shared

Schools, local education authorities and the Department for Education (DfE) all hold personal information on pupils in order to run the education system, and in doing so have to follow the Data Protection and related Acts. This means, among other things that the personal data held must only be used for specific purposes allowed by law. The school has a Privacy Notice which explains how personal data is used and with whom it will be shared. This Notice is published here:

https://www.birchcopse.co.uk/gdpr

The Privacy Notice is reviewed annually to ensure it reflects current data processing and data sharing arrangements

Processing, storing, archiving and deleting personal data: guidance

- Personal data and school records about pupils are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change schools.
- School records for a child, including photographs, are kept for seven years after the child leaves the school unless subject to legal hold and or for children with special educational needs.
- Data on staff is sensitive information and confidential to the individual. It is only shared, where appropriate, at the discretion of the Head Teacher and with the knowledge, and if possible, the agreement of the staff member concerned. This includes data on school-provided e-mail system.
- Employment records form part of a staff member's permanent record. Because there are specific legislative issues connected with these (salary and pension details etc.). These records should be retained as set out by the Local Authority
- Interview records, CVs and application forms for unsuccessful applicants are kept for 6 months.
- All formal complaints made to the Head Teacher or Governing Board will be kept for at least seven years in confidential files, with any documents on the outcome of such complaints. Individuals concerned in such complaints may have access to such files subject to data protection processes and to legal professional privilege in the event of a court case.
- All members of staff should only access school-provided systems (including e-mail) up to the last day of employment.
- Retention and disposal of records is carried out in line with the Information and Records Management Society's (IRMS) Toolkit for Schools, unless there are specific legal or statutory requirements which require a different approach.

Accessing personal data: guidance

- A pupil may request access to their own personal data. Requests may be made verbally or in writing. The school will consider each request on a case-by-case basis, taking into account the child's age, maturity and ability to understand the nature of the request and the information involved. Staff may assist pupils in making a request where appropriate. Any concerns regarding coercion or safeguarding will be considered and decisions will be documented.

- A parent can request access to or a copy of their child's school records and other information held about their child. The request must be made in writing. There is no charge for such requests on behalf of the child, but there may be an agreed charge for photocopying records. Staff should check, if a request for information is made by a parent, that no other legal obstruction (for example, a court order limiting an individual's exercise of parental responsibility) is in force.
- Parents should note that all rights under the Data Protection Act to do with information about their child rest with the child as soon as they are old enough to understand these rights. This will vary from one child to another. In a primary school setting, parents will normally act on behalf of their child, although older pupils may sometimes be involved in decisions about access to their information where appropriate.
- Separately from the Data Protection Act, The Education (Pupil Information) (England) Regulations 2005 provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. Parents who wish to exercise this right must apply to the school in writing.
- For educational records (unlike other personal data; see below) access must be provided within 15 school days, and if copies are requested, these must be supplied within 15 school days of payment of the cost of copying.
- A member of staff can request access to their own records at no charge, but the request must be made in writing. The member of staff has the right to see their own records, and to ask for copies of the records. There is no charge for copies of records.
- Requests for personal data will usually be responded to within one month of receipt. Where requests are complex or numerous, the school may extend this period by up to a further two months but will inform the requester of this within one month, except requests for educational records (see above) or with agreement with the Data Subject.
- All requests will be acknowledged in writing on receipt within a working week, and access to records will be arranged as soon as possible. If awaiting third party consents, the school will arrange access to those documents already available and notify the individual that other documents may be made available later.
- In all cases, should third party information (information about another individual) be included in the information the school will try to obtain permission from the third party to show this information to the applicant. If third party permission is not obtained the person with overall responsibility should consider whether the information can still be released.
- Personal data should always be of direct relevance to the person requesting the data. A document discussing more general concerns may not be defined as personal data.
- Under the Freedom of Information Act, a request for personal information can include unstructured as well as structured records – for example, letters, emails etc. not kept within an individual's personal files, or filed by their name, but still directly relevant to them. If these would form part of a wider record it is advisable to file these within structured records as a matter of course and to avoid excessive administrative work in the future.
- Anyone who requests to see their personal data has the right to question the accuracy of matters of fact within the data, and to ask to have inaccurate information deleted or changed. They may also question opinions, and their comments will be recorded, but opinions do not need to be deleted or changed as a part of this process.
- The school will document all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes (letter requesting changes etc.) This will enable staff to deal with a complaint if one is made in relation to the request. If no complaint is received, these records will be deleted at the same time as the related personal records.

Examples of good practices

- Only school-provided data storage (which are centrally archived/encrypted) should be used to store work-related personal data. No USB pen is to be used for storing personal data.
- Personal data should only be accessed using secure and password-protected internet connections.
- Do not open uninvited e-mail from unrecognised source – check its source with a phone call or delete the mail item without opening any attachment / click on any links.
- Only use computers which have operational anti-virus software.
- Use secure e-mail tool where available by default for all communication involving personal data.
- Personal data must only be stored on school-approved, encrypted systems such as Google Workspace or other authorised platforms, not on personal devices or unencrypted drives.
- Staff should avoid using pupils' full names in email subject lines or filenames unless necessary for safeguarding or operational reasons.
- Holder of passwords should learn how to change the passwords without the help of a third person. Experiences have shown that damages could have been limited when password is changed as and when leakage is noticed.
- Do not use your school email address to authenticate online resources without agreement with the school. You are increasing the exposure of your account to uninvited attention.
- Look out for unexpected behaviour of your computer – if in doubt, check with a colleague.
- Get to know the steps you need to follow when personal data is lost / leaked to the open world.
- Practice what we preach – children would pick up good practices from us – it is their future we are working to safeguard.