Beenham Primary School

Data Protection and GDPR
POLICY DOCUMENT

Aims & Objectives:

The aim of this policy is to provide a set of guidelines to enable all members of staff 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 Beenham Primary School acts within the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 when retaining and storing personal data, and when making it available to individuals.

Data Protection – the law:

Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, access to 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.

School staff have a right of access to personal data on themselves. - 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. The Headteacher has operational responsibility for data protection compliance within the school. The Governing Board retains overall accountability.

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 amount of personal data is 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; image 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 information on pupils in order to run the education system, and in doing so have to follow the Data Protection and Data Protection policy. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law. The school has a Fair Privacy Notice which explains how personal data is used and with whom it will be shared.
This Notice is published here: www.beenhamprimary.co.uk

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.
- The school follows the Information and Records Management Society (IRMS) Toolkit for Schools retention schedule. Retention periods vary depending on the type of record.
- 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 School Governors 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 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.

CCTV and video surveillance

The school operates CCTV for specified purposes which may include safeguarding pupils, staff and visitors; maintaining the security of the school premises; preventing and investigating crime, vandalism and unauthorised access; protecting school property; and assisting with the investigation of serious incidents where the use of CCTV footage is necessary and proportionate.

Images and recordings of identifiable individuals constitute personal data and will therefore be processed in accordance with the UK GDPR, the Data Protection Act 2018 and the school's data protection policies and procedures.

CCTV footage will only be accessed by authorised individuals and will be retained only for as long as is necessary for the purposes for which it was collected. Routine recordings are normally retained for 30 days before being automatically overwritten or securely deleted, unless particular footage needs to be retained for longer in connection with an incident, safeguarding matter, complaint, investigation, insurance claim or legal proceedings.

Further information about the operation and management of the school's CCTV system is contained within the school's CCTV Policy.

Accessing personal data: guidance

All subject access requests (SARs) will be handled in accordance with UK GDPR.
The school will respond within one calendar month of receipt, subject to permitted extensions where requests are complex or numerous.
The school may request proof of identity before releasing information.

● A child can request access to his/her own data. All subject access requests (SARs) will be logged formally by the school, regardless of whether they are received verbally or in writing. While a request does not need to be submitted in writing, the school may confirm the scope of the request in writing to ensure clarity. No fee will be charged unless the request is manifestly unfounded or excessive, in accordance with UK GDPR. All decisions should 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 subject access requests unless the request is manifestly unfounded or excessive. For educational record requests made under the Education (Pupil Information) (England) Regulations 2005, a reasonable fee may be charged for copies in line with those Regulations.

● 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, but, as a broad guide, it is reckoned that most children will have a sufficient understanding by the age of 12. Parents are encouraged to discuss and explain any request for information with their child if they are aged 12 or over.

● 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.

● GDPR requires that all requests for personal information are dealt with within 1 month of receipt except requests for educational records (see above) or with agreement with the Data Subject.

All requests will be acknowledged in writing on receipt, 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 staff 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.

● Requests for an individual's own personal data are handled under UK GDPR. Freedom of Information Act requests apply to non-personal information held by the school.

● 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.

Personal Data Breaches

All personal data breaches must be reported immediately to the Headteacher and the Data Protection Officer. The DPO will assess whether the breach meets the threshold for reporting to the Information Commissioner's Office within 72 hours and whether affected individuals must be informed.

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.
- Avoid using unknown supplier of Wi-Fi services for work activities which involve personal data.
- 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.
- Look out for unexpected behaviour of your computer – if in doubt, check with a colleague.
- Log queries as questions for your next CPD – everything has an explanation.
- Work to separate (storage of) personal and non-personal data as and when data are being worked on.
- 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.

Change History

Version	Date	Change
2.0	March 2026	Provided detailed compliance amendments including lawful basis clarification, retention schedule alignment, SAR procedure update, breach reporting inclusion, and removal of outdated legislative references prior to governor approval. Final compliance review of GDPR Privacy Notice and Data Protection and GDPR Policy completed prior to governing board approval. Documents confirmed aligned with UK GDPR, Data Protection Act 2018, IRMS retention guidance and ICO breach reporting expectations.
3.0	September 2026	Added CCTV and video surveillance section.

Approved by: Full Governing Board
Date approved: October 2026
Review date: September 2027