Batchwood School Data Protection Policy

Policy owner: Data Protection Officer (DPO) – Mrs Katie Harris

Day-to-day data protection queries: head@batchwood.herts.sch.uk

Applies to: All staff, governors, contractors, volunteers and external processors working on behalf of the school.

Ross Whitaker

…… ……

Signed – Headteacher **Print Name**

Date reviewed: June 2026
Next review due: June 2027

Contents

1. Policy Statement and Scope

To function properly, Batchwood School collects and uses certain types of information about staff, pupils, parents/carers, governors, contractors, visitors and other individuals who come into contact with the school. We are also required to collect and share data to fulfil our statutory obligations to the Local Authority (LA), the Department for Education (DfE) and other bodies. Personal information must be handled lawfully, fairly and securely—whether recorded on paper, in a computer system or by other means. This policy sets out how we comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data the school processes, regardless of format (paper or electronic). It does not form part of any employee's terms and conditions and may be amended from time to time. All members of staff must familiarise themselves with and follow this policy.

2. Legal Framework

This policy is based on the UK GDPR and the DPA 2018 and reflects guidance from the Information Commissioner's Office (ICO), including the Surveillance Camera Code of Practice as it relates to personal information. It also complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 regarding parental access to a child's educational record.

3. Definitions

Personal data: Any information relating to an identified or identifiable living individual (a 'data subject'), such as name (including initials), identification number, location data, online identifiers (e.g. usernames), or factors specific to physical, physiological, genetic, mental, economic, cultural or social identity.

Special category data: Personal data needing extra protection, including information about racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetics; biometrics (where used for identification); health (physical or mental); sex life or sexual orientation.

Processing: Any operation performed on personal data, automated or manual (e.g. collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, disclosure, dissemination, erasure or destruction).

Data subject: The identified or identifiable individual to whom the personal data relates.

Data controller: The person or organisation that determines the purposes and means of processing personal data. The school is the data controller for most processing activities.

Data processor: A person or organisation (other than the controller's employee) processing personal data on behalf of the data controller.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Roles and Responsibilities

Governing Board: Has overall responsibility for ensuring the school complies with data protection obligations.

Headteacher: Acts as the representative of the data controller on a day-to-day basis.

Data Protection Officer (DPO): Oversees implementation of this policy, monitors compliance with data protection law, and develops related policies and guidance as needed. Provides an annual report to the governing board and acts as first point of contact for data subjects and the ICO. DPO: Mrs Katie Harris – gdprkharris@gmail.com.

All staff: Must collect, store and process personal data in accordance with this policy; keep their own personal data up to date; and contact the DPO with any questions or concerns, when relying on/recording consent, drafting privacy notices, handling data protection rights, transferring data internationally, reporting a suspected breach, engaging in new activities that may affect privacy, or when sharing data with third parties.

5. Data Protection Principles

We fully endorse and adhere to the data protection principles. Personal data must be: (1) processed lawfully, fairly and transparently; (2) collected for specified, explicit and legitimate purposes; (3) adequate, relevant and limited to what is necessary; (4) accurate and, where necessary, kept up to date; (5) kept no longer than necessary; and (6) processed securely. We also ensure accountability by documenting and evidencing our compliance.

6. Lawful Bases and Fairness

We will only process personal data where at least one lawful basis applies: contract; legal obligation; vital interests; public task (as a public authority); legitimate interests (where appropriate and not overridden by data subject rights); or consent. For special category data, a separate condition under data protection law will also be met (e.g. explicit consent; employment/social protection; vital interests; manifestly public; legal claims; substantial public interest; health or social care; public health; archiving/research/statistics in the public interest). For criminal offence data, we will meet both a lawful basis and a relevant condition in data protection law.

We will consider fairness and transparency in all processing, ensuring individuals would reasonably expect the way we use their data and that we avoid unjustified adverse effects.

7. Collecting Personal Data: Limitation, Minimisation and Accuracy

We collect personal data for specified, explicit and legitimate purposes and explain these purposes when data is first collected (via privacy notices). If we wish to use personal data for a new purpose, we will inform individuals beforehand and seek consent where required. Staff shall only process the personal data necessary for their role, keep data accurate and up to date, and delete or anonymise data when no longer needed in line with our records retention schedule.

8. Sharing Personal Data

We do not normally share personal data without consent. However, we may share data where required or permitted by law, for example: to protect staff or pupil safety; to liaise with other agencies (seeking consent as necessary); with suppliers/contractors to provide services (subject to due diligence, appropriate contracts and sharing only what is necessary); with law enforcement and government bodies where legally required; and with emergency services/local authorities in response to incidents.

Where we transfer personal data internationally, we will do so in accordance with data protection law, ensuring appropriate safeguards for transfers outside the UK (and, where EU GDPR applies, outside the EEA).

9. Rights of Individuals

Individuals have rights which may include: to be informed; to access their data; to rectification; to erasure; to restrict processing; to data portability; to object; to withdraw consent; to challenge decisions based solely on automated processing or profiling; and to be notified of certain personal data breaches. Requests to exercise these rights should be submitted to the DPO. Staff must forward any such request to the DPO immediately.

10. Subject Access Requests (SAR)

Individuals may request confirmation that their data is processed and access to their personal data and related information (e.g. purposes, categories, recipients, retention, rights, source, any automated decision-making, and international transfer safeguards). Requests can be made in any form, but we can respond faster if made in writing and include the individual's name, correspondence address, contact details and a description of the information requested. Staff must forward all SARs to the DPO without delay.

We may request identification, confirm the request by phone, and will respond without undue delay and within one month of receipt (or of receiving any additional identity information). We may extend by up to two further months for complex or numerous requests, informing the requester within one month and explaining why. Information will normally be provided free of charge. We may refuse or charge a reasonable fee where a request is unfounded or excessive

(including repetitive requests); if refused, we will explain why and inform the individual of their right to complain to the ICO or to court.

We may withhold information where disclosure would: cause serious harm to the physical or mental health of the pupil or another person; reveal that a child is at risk of abuse where disclosure would not be in their best interests; include another person's personal data which cannot reasonably be anonymised and consent has not been given; or form part of certain sensitive documents (e.g. related to crime, immigration, legal proceedings, legal professional privilege, management forecasts, negotiations, confidential references or exam scripts).

11. Children and Subject Access Requests

Personal data about a child belongs to the child. Parents/carers may exercise a SAR on behalf of a child if the child is not competent to understand their rights and the implications of a SAR, or with the child's consent. As a guide, children aged 12 and over are generally considered mature enough to understand their rights, but competence is assessed case by case.

12. Parental Requests to See the Educational Record

Parents or those with parental responsibility have a statutory right to free access to their child's educational record (which covers most information about a pupil) within 15 school days of a written request, for pupils under 18. A reasonable fee may be charged for copies. In some cases, the right can be denied, for example if release might cause serious harm to the physical or mental health of the pupil or another individual or would reveal exam marks before they are officially announced.

13. CCTV

We use CCTV in various locations on site to help keep the school safe. We follow applicable codes of practice. Cameras are clearly visible and signage explains that CCTV is in operation. Enquiries should be directed to admin@batchwood.herts.sch.uk.

14. Photographs and Videos

As part of school activities, we may take photographs or record images. We obtain written consent from parents/carers (or from pupils aged 18 and over) for communication, marketing and promotional materials and explain clearly how images will be used. Photos/videos taken by parents/carers for personal use at school events are generally outside data protection law; however, for safeguarding reasons, we ask that images including other pupils are not shared publicly unless the relevant parents/carers (or pupils, where appropriate) have agreed.

Where the school takes photographs or videos, uses may include: within school (e.g. noticeboards, magazines, brochures, newsletters), outside the school by external agencies (e.g.

school photographer, press), and online (e.g. website, social media). Consent may be withdrawn at any time, in which case we will delete the image/video and cease further distribution. We do not publish additional personal information alongside images that could identify a child.

15. Data Protection by Design and Default

We integrate data protection into our processing by: appointing a suitably qualified DPO with adequate resources; limiting processing to what is necessary for each purpose; completing Data Protection Impact Assessments (DPIAs) where processing presents high risks or when introducing new technologies; embedding data protection into policies and privacy notices; providing regular staff training and keeping attendance records; conducting reviews and audits of privacy measures; and maintaining records of processing activities. Where we transfer personal data outside the UK (and, where EU GDPR applies, outside the EEA), appropriate safeguards will be in place.

16. Data Security and Storage of Records

We keep personal data secure against unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Measures include: keeping paper records and portable devices containing personal data locked away when not in use; not leaving papers containing personal data unattended; signing out/in personal information taken off site; using strong passwords (minimum 10 characters, including letters and numbers) and avoiding reuse from other sites; encrypting portable devices and removable media; ensuring anyone storing school personal data on a personal device follows the same security standards; and conducting due diligence when sharing data with third parties to ensure secure storage and adequate protection.

17. Disposal of Records

Personal data that is no longer needed or has become inaccurate or out of date and cannot be rectified will be disposed of securely. Paper records will be shredded or incinerated and electronic files overwritten or securely deleted. Where third parties are used for disposal, we will obtain sufficient guarantees of compliance with data protection law.

18. Personal Data Breaches

We will make all reasonable endeavours to prevent personal data breaches. In the event of a suspected breach, we will follow the procedure in Appendix 1. Where appropriate, we will notify the ICO within 72 hours of becoming aware of a reportable breach. Examples of breaches in a school context include (but are not limited to): non-anonymised datasets published online; safeguarding information disclosed to an unauthorised person; or theft of an unencrypted device containing personal data.

19. Training

All staff and governors receive data protection training as part of induction and through ongoing CPD when legislation, guidance or internal processes change.

20. Monitoring and Review

The DPO is responsible for monitoring and reviewing this policy. It will be reviewed at least every two years and shared with the full governing board.

Appendix 1: Personal Data Breach Procedure

This procedure is based on ICO guidance on personal data breaches.

• On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
• The DPO will investigate and determine whether a breach has occurred by considering whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed or made available to unauthorised people.
• The DPO will alert the headteacher and the chair of governors.
• The DPO will contain and minimise the impact, assisted by relevant staff or processors as necessary.
• The DPO will assess potential consequences (severity and likelihood) and whether the breach must be reported to the ICO (judged case by case, considering risks to rights and freedoms such as loss of control, discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality or other significant disadvantage). If risk is likely, the ICO will be notified.

• The DPO will document the decision in all cases. Records are stored on Batchwood School's shared drive in a GDPR folder restricted to authorised persons.
• Where notification to the ICO is required, the DPO will report via the ICO 'report a breach' service or breach line (0303 123 1113) within 72 hours, including: (a) description of the breach and categories/approximate numbers of individuals and records; (b) DPO contact details; (c) likely consequences; and (d) remedial/mitigation measures taken or proposed. If full details are not yet known, an initial report will be submitted within 72 hours with reasons for delay and timelines for the remaining information.

• The DPO will assess the risk to individuals; if high, the DPO will promptly inform in writing all affected individuals with plain-language information about the breach, the DPO's contact details, likely consequences, and measures taken or proposed.
• The DPO will notify relevant third parties who can help mitigate loss to individuals (e.g. police, insurers, banks, credit card companies).
• Each breach will be documented with facts, effects and actions taken to contain and prevent recurrence (e.g. process improvements or further training). Records will be stored on Batchwood School's shared drive in a GDPR folder restricted to authorised persons.
• The DPO and headteacher will meet as soon as reasonably possible to review the incident and lessons learned.

Actions to minimise the impact of different breach types include (non-exhaustive):
• Special category data disclosed via email (e.g. safeguarding records): the sender must attempt to recall the email immediately; recipients must alert the sender and DPO; if recall fails, ICT will attempt recall; where unsuccessful, the DPO will contact recipients to request deletion and non-disclosure, obtain written confirmations, and conduct internet searches to ensure the information has not been made public, contacting site owners for removal if necessary.
• Non-anonymised pupil premium interventions or exam results published online: remove

content immediately, inform affected individuals where appropriate, and review publication approval workflows.

• Sensitive personal data on an unencrypted device stolen or hacked: notify IT to trigger remote wipe (where possible), inform affected individuals where risk is high, and review encryption and asset controls.

• Third-party provider breach (e.g. cashless payment provider): obtain incident details and assurances, coordinate notifications where required, and review supplier due diligence and contract clauses.