



Blossom House School

Station Road, Motspur Park
New Malden, KT3 6JJ
United Kingdom

+44 (0)20 8946 7348
mpadmin@blossomhouseschool.co.uk
www.blossomhouseschool.co.uk

Data Protection Policy

EYFS, Adapted Curriculum, Primary, Secondary and P16
Motspur Park, Euston and Wimbledon

Independent advisor: Satswana Ltd, Data Protection Officer

Operational management: DP Committee

Updated: September 2026

To review: September 2027



MOTSPUR PARK | EUSTON | WIMBLEDON

Principal: Joanna Burgess OBE, MRCSLT, Dip. RSA SpLD, PGCE, HCPC
Registered Office: Station Road, Motspur Park, New Malden, KT3 6JJ, UK

Blossom House School Ltd
Registered in England no. 5198780

This policy sets out how Blossom House School protects personal information while delivering education, therapy, care and safeguarding. It explains the responsibilities of school personnel and the procedures for information sharing, requests, complaints, security incidents and new technology.

Principal changes

The redraft retains the school's committee and co-ordinator structure while updating the legal framework, children's information, rights handling, complaints, automated decisions, technology assessment and UK international transfers. Named committee members are replaced by roles. The six-monthly committee meeting cycle is retained.

Contents

- 1 Purpose and scope
- 2 Key terms
- 3 Governance and responsibilities
- 4 Data protection principles
- 5 Lawful use and consent
- 6 Transparency and fair handling
- 7 Children and school information
- 8 Records accuracy and retention
- 9 Information security
- 10 Personal data breaches
- 11 Subject access and other rights requests
- 12 Data protection complaints
- 13 Sharing information and using suppliers
- 14 UK international transfers
- 15 Data protection by design and new technology
- 16 Automated decisions and profiling
- 17 Communications marketing and online services
- 18 Accountability training and review
- Appendix A School confirmation and approval checklist
- Appendix B Legal and guidance references

Select a contents entry to go to that section. Word's Navigation Pane also lists the policy headings.

Staff quick reference

Suspected breach: report immediately and preserve evidence.

Request for information or complaint: forward immediately; record when received.

Safeguarding concern: follow the safeguarding procedure without delay.

New supplier, system, AI tool or overseas access: seek approval before use.

1 Purpose and scope

Blossom House School will use personal information lawfully, fairly, transparently and securely. Protecting pupils and respecting their privacy are complementary responsibilities. Data protection must support timely, justified safeguarding and the delivery of suitable education and therapy. This policy applies across Motspur Park, Euston and Wimbledon and to EYFS, Adapted Curriculum, Primary, Secondary and Post 16 provision. It covers information about prospective, current and former pupils, parents and carers, personnel, applicants, visitors, suppliers and other individuals. References to children mean those under 18; adult learners retain their own rights.

All employees, workers, agency staff, volunteers, apprentices, consultants, contractors, leaders and other authorised personnel must follow this policy when handling information for the school. It covers paper records, email, messaging, photographs, recordings, cloud services, school systems and authorised remote working. Confidentiality obligations continue after a person leaves. The school complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025 (DUAA), and with the Privacy and Electronic Communications Regulations 2003 (PECR) where applicable. This policy is read alongside current safeguarding requirements, including Keeping Children Safe in Education 2026. References to legislation include amendments in force. [1–3, 13]

The controller is the legal entity determining why and how the information is used. The school's main correspondence address is Station Road, Motspur Park, New Malden, KT3 6JJ. Controller responsibilities are not transferred to the DPO, suppliers or individual employees. This policy may be shared with families, personnel, regulators and other interested people. Security-sensitive procedures and personal information within supporting records remain appropriately restricted. Privacy notices explain particular uses of information; this policy does not replace those notices.

2 Key terms

Personal data is information relating to an identified or identifiable living person, including opinions, identifiers and information inferred about them. Processing includes collecting, viewing, recording, changing, sharing, storing and deleting it. A data subject is the person the information concerns.

Special category data includes health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data used for unique identification, and sex life or sexual orientation. Criminal offence data is a separate category covering convictions, offences and related security measures, including relevant allegations. [1] A processor handles personal data on the controller's behalf and instructions. A separate controller determines its own purposes and means; joint controllers determine them together. The actual activity, rather than a contract label, determines each party's role. Pseudonymised information remains personal data where a person can be identified using additional information. Information is anonymous only where identification is not reasonably likely. Removing a name alone rarely anonymises a detailed pupil or therapy record.

3 Governance and responsibilities

3 1 Leadership and the Data Protection Committee

The Proprietor is Blossom House School. The Principal is also the senior accountable lead and ensures urgent decisions can be made without waiting for a committee meeting.

The Data Protection Committee, overseen by the IT Department retains the operational oversight function previously described as Data Protection Manager. Its proposed role-based membership, reflecting the existing policy, is: School Principal; Head of Administration; Designated Safeguarding Lead; IT Managers; Head of Therapies; Euston School leads, Wimbledon leads; and Human Resources manager.

The Committee oversees implementation, information risks, training, retention, supplier arrangements, rights requests, complaints, incidents and improvement actions. It meets at least every six months and more often when necessary. Decisions, assigned owners, deadlines and completion evidence must be recorded. Urgent safeguarding, incident and statutory deadline decisions must be escalated immediately.

3 2 Data Protection Co-ordinator

The IT Department acts as Data Protection Co-ordinator, specifically Alban Sejdiu and Connor Lasic. The Co-ordinators work with Satswana Ltd, arranges six-monthly meetings, circulates actions and follows up completion. They maintain the central compliance registers and contact directory, allocate requests promptly, track deadlines and arrange cover during absence and holidays. The Co-ordinator does not replace the independent DPO.

3 3 Data Protection Officer

Satswana Ltd is the DPO identified in the existing policy. The recorded contact details are info@satswana.com and 01252 759177. People may contact the DPO directly and confidentially about the use of their information. The DPO advises on compliance and DPIAs, monitors compliance, supports training and audits, and acts as a contact for individuals and the ICO. The school must involve the DPO early, provide access and resources, protect their independence and avoid conflicts of interest. The DPO reports to the highest management level. Management retains decisions and accountability; reasons for departing from DPO advice must be recorded.

3 4 Departmental leads and all personnel

IT leads manage technical security, access controls, recovery and supplier technical checks. HR leads oversee recruitment and workforce records. Administration leads oversee admissions, family communications and administrative records. The Head of Therapies oversees therapy information and professional confidentiality. The Designated Safeguarding Lead (DSL) oversees child protection information and urgent safeguarding disclosures. Each department owns the accuracy, access and retention of its records.

Personnel must complete training, use only authorised systems, access information only for work they are authorised to perform, and immediately report incidents, rights requests and complaints. They must seek advice before introducing a new use, supplier, overseas access arrangement or technology, or whenever lawful basis, consent, retention or disclosure is unclear. A line manager's absence must not delay escalation.

4 Data protection principles

The school must be able to demonstrate compliance with these principles:

- Lawfulness, fairness and transparency: use an appropriate legal basis, treat people fairly and explain how their information is used.

- Purpose limitation: specify legitimate purposes and assess any proposed further use before proceeding.
- Data minimisation: collect and share information that is adequate and relevant, limited to what the purpose requires.
- Accuracy: take reasonable steps to keep information accurate and current and rectify or erase inaccurate information without delay where appropriate.
- Storage limitation: retain identifiable information only for as long as it is needed for a justified purpose.
- Integrity and confidentiality: protect against unauthorised or unlawful processing and accidental loss, destruction or damage.
- Accountability: maintain evidence of the decisions, controls and checks used to meet these requirements.

5 Lawful use and consent

5 1 Selecting and recording a lawful basis

Before starting processing, the department lead must record its purpose and Article 6 basis in the processing register, with DPO advice where needed. The basis must fit the specific activity and the individual concerned. A parent's fee contract does not automatically provide a contract basis for processing the child's information. Nor does independent school status automatically establish a public task. [1, 4] Available bases include consent; necessity for a contract with the individual or requested pre-contract steps; legal obligation; vital interests; a task in the public interest or official authority grounded in law; ordinary legitimate interests; and a recognised legitimate interest within the statutory list. Record the relevant legal obligation or function when relying on it. Vital interests are reserved for protecting life, not routine administration.

For ordinary legitimate interests, complete a documented assessment of purpose, necessity and the balance with the person's rights, giving particular weight to children and vulnerable people. For recognised legitimate interests, confirm the precise statutory condition and necessity; the absence of a balancing test does not remove fairness, transparency or other safeguards. The DPO must review any proposed reliance on this newer basis. [4]

5 2 Special category and criminal offence data

An Article 6 basis alone is insufficient for special category data. The school must also document an applicable Article 9 condition and any required DPA 2018 Schedule 1 condition. Depending on the activity, these may concern employment obligations, health or social care under appropriate confidentiality duties, substantial public interest including safeguarding, legal claims or valid explicit consent. None is a blanket permission for all school information. [1, 2] Health, disability, SEND assessments, education health and care plans (EHCPs), therapy notes, medication, mental health and safeguarding records require particular care. The Head of Therapies and DSL must help define who needs access and what information other staff need to act safely. Staff should receive relevant practical support information without unnecessary access to an entire clinical or safeguarding file.

Criminal offence information, including relevant vetting and allegation records, requires Article 10 authority as well as an Article 6 basis. The school must identify the applicable DPA 2018 condition. Where required, an appropriate policy document must explain compliance safeguards and retention and erasure arrangements. It must be maintained and made available

to the ICO on request. DBS information must follow the applicable statutory and DBS handling rules.

5 3 Using consent appropriately

Consent must be freely given, specific, informed and unambiguous, expressed by a positive action. Explicit consent needs an express statement. Staff must record what was agreed, by whom, when and how, including the information provided. Pre-ticked boxes, silence and bundled permissions are not acceptable. Consent should not be used where refusing would cause an unfair disadvantage, or the school must process the information regardless. People must be able to withdraw consent as easily as they gave it. Stop the consent-based activity promptly after withdrawal; earlier lawful processing is unaffected. Do not change the stated basis merely to evade withdrawal. Separate optional publicity permissions from essential educational and safeguarding uses. Consider the pupil's understanding and wishes and parental authority where appropriate; there is no single age threshold for all school consent decisions.

6 Transparency and fair handling

The school will:

provide clear privacy notices for pupils and families, applicants and personnel, and other relevant groups. Use accessible language and formats, including supported explanation where needed. Notices must identify the controller and DPO, purposes and legal bases, legitimate interests where relevant, recipients, international safeguards, retention, rights and complaint routes, including the right to complain to the school. Explain required information and the consequences of not supplying it, and relevant automated decisions. [1, 5] Provide the notice when collecting information directly. When obtaining information elsewhere, provide the Article 14 information, including its categories and source, within a reasonable period and at the latest one month, or earlier at first communication or disclosure if applicable. The DPO must assess and record any statutory exception; do not assume safeguarding creates a general transparency exemption. A new purpose requires a documented assessment of lawfulness, compatibility under the current UK GDPR provisions, fairness and transparency, and updated notices before further use where required. Compatibility alone is not a lawful basis. Information that is publicly available remains subject to data protection requirements.

7 Children and school information

7 1 Supporting pupils and respecting their rights

Personnel must take account of pupils' age, development, communication needs, SEND and other vulnerabilities without assuming that disability removes the ability to understand or exercise rights. Provide suitable assistance, accessible explanations and an opportunity to express views. The interests of a child require particular weight when assessing fairness, necessity and risk. Parents and carers do not automatically have unrestricted access to every pupil record. Check identity, parental responsibility or other authority, the pupil's competence and wishes, court orders, confidentiality and safeguarding concerns. A competent child may exercise their own rights or authorise a representative. For an adult learner, parental status alone does not authorise access; consider consent, lawful authority and any relevant capacity framework. Educational and therapy observations must distinguish fact, professional opinion and unverified reports. Record sources, dates, author and relevant context. Correct factual errors and record a disputed view appropriately without erasing a necessary audit trail or altering an honestly held historical professional opinion.

7 2 Safeguarding and multi-agency sharing

Data protection does not prevent necessary and proportionate sharing to protect a child. Personnel must follow the safeguarding policy and refer concerns promptly to the DSL or deputy. In an emergency, contact the appropriate emergency or safeguarding service without waiting for data protection clearance, and document and report the disclosure as soon as possible. [13, 14]

Consent is not normally the appropriate basis where sharing is required to safeguard a child. The DSL, with DPO advice where useful, must identify the Article 6 basis and any Article 9, Article 10 and DPA conditions. Share relevant, accurate information securely with verified recipients. Consider whether informing the family could increase risk or prejudice protective action; record any decision not to inform them. Record what was shared, with whom, why, when, the lawful basis and any restrictions, or why a decision was made not to share. A missing routine sharing agreement must not prevent urgent lawful safeguarding. Child protection files must be separately secured and transferred with confirmation of receipt in accordance with current safeguarding guidance and the school's safeguarding procedure.

The DSL must review local sharing arrangements for the information sharing duty under section 16LA of the Children Act 2004, due to commence on 30 September 2026, and apply the duty and associated statutory guidance when it applies

7 3 Images and monitoring

Use school-approved devices and storage for photographs, audio and video, including therapy recordings. Define the purpose, access and deletion period before recording. Check permissions and restrictions before publication, avoid unnecessary identification or location details, and provide an effective route to change optional publicity choices. Safeguarding restrictions take priority over general publicity permissions.

CCTV, filtering and monitoring, location tools, biometrics and other monitoring must be necessary, proportionate, transparent and approved following the assessment in section 15. Restrict access and routinely delete recordings under the retention schedule, preserving relevant evidence when needed. Biometric identification of pupils requires assessment of the Protection of Freedoms Act 2012 requirements, including parental notification and written consent where applicable, the child's right to object and an alternative service. No system may be introduced merely because a supplier offers it.

8 Records accuracy and retention

Department leads must use the approved retention schedule, which must cover pupil and admissions records, SEND and therapy records, safeguarding, recruitment and employment, finance, complaints, incidents, communications, recordings and system logs. Each entry must state the purpose, owner, retention period, trigger date, justification and disposal method.

Do not apply a single period to every record or keep information indefinitely because storage is available. Different obligations may apply to clinical, safeguarding and employment records. Set review dates for records with uncertain continuing need and seek advice before disposal where safeguarding, professional duties, litigation, an inquiry or a statutory retention requirement may apply. A documented preservation hold must suspend relevant routine deletion when required for a request, complaint, investigation, claim or inquiry. The responsible lead must identify the records, access restrictions and review date, and formally

release the hold when appropriate. Personnel must never destroy, conceal or alter information to prevent a lawful disclosure.

Dispose of records securely, including copies, downloads, removable media and processor-held information. Use confidential destruction for paper and verified secure erasure or destruction for equipment. Keep appropriate disposal evidence. Where immediate removal from backup is not practicable, put the data beyond ordinary use, expire it under a defined cycle and prevent its inappropriate restoration into live use.

9 Information security

IT and department leads must maintain safeguards proportionate to the risks, with particular attention to sensitive pupil information. Controls must protect confidentiality, integrity and availability and support safe continuity of education, therapy and safeguarding.

- Give each user an individual account and the minimum access needed. Approve access, review it regularly and remove or adjust it promptly when roles change or people leave. Use strong authentication, including multi-factor authentication where appropriate to risk.
- Use supported, updated systems, anti-malware protection, secure configurations and suitable encryption for devices, storage and transmission. Protect backups, separate them appropriately and test restoration and incident recovery.
- Use approved school accounts, devices, storage and transfer methods. Personal email, consumer messaging, unapproved cloud storage and removable media must not be used for school information without specific authorisation and safeguards.
- Check recipients and attachments before sending them. Use secure transfer for sensitive or extensive records. Do not expose distribution lists unnecessarily; use approved mailing tools or appropriate BCC controls for non-sensitive bulk messages.
- Keep paper files and portable devices secure, lock screens, retrieve printing promptly, protect conversations from being overheard and limit records taken off site. Report lost devices or papers immediately.
- Protect remote working and remote supplier access. Maintain appropriate logs, review suspicious activity and report phishing, misdirected communications and unauthorised access. Never share passwords or bypass safeguards.

Managers must ensure that staff can find the current IT, acceptable use, remote working and incident procedures. Monitoring of staff must itself be lawful, proportionate and explained.

10 Personal data breaches

A personal data breach is a security failure causing accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. It can include lost paper files, a misdirected email, unauthorised access, ransomware or loss of availability. A near miss must also be reported so that weaknesses can be addressed.

10.1 Immediate action

Personnel must report a suspected or actual breach immediately to the Data Protection team and the senior duty lead, and alert IT and the DSL where relevant. Use the operational contact directory in section 18; if unavailable, contact the Principal or Head of Operations and the DPO directly. Do not wait for certainty, a manager's return or a committee meeting. Preserve messages, logs and other evidence. Take safe containment steps within your authority, but do not conduct an unauthorised investigation or delete evidence.

10 2 Assessment and notifications

The Principal or delegated incident lead will co-ordinate containment and recovery, involve the DPO promptly and record when the school became aware. Assess the affected people and information, scale, sensitivity, possible misuse and consequences, including risks to a child's safety, confidentiality, wellbeing or access to care. The school must notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to result in a risk to people's rights and freedoms. Weekends and holidays count. Do not wait for a complete investigation: provide an initial report and further information in phases, and explain any delay. [10]

Where a breach is likely to result in a high risk, inform affected people without undue delay in clear, accessible language, unless a statutory exception applies and is documented with DPO advice. Explain the nature of the breach, likely consequences, protective action, measures taken and a contact point. Consider carefully how to communicate with pupils and families without adding safeguarding risk. Other reporting duties and safeguarding referrals must be assessed separately. The breach register must record every personal data breach, its effects, risk assessment, notification decisions and reasons, remedial action and lessons learned, including breaches not reported to the ICO. The incident lead assigns improvements and completion dates. The Committee reviews trends. Suppliers must report breaches to the school without undue delay; contractual escalation must allow the school to meet its own deadlines.

11 Subject access and other rights requests

11 1 Recognising and allocating requests

A request can be verbal or written, made to any member of personnel and need not cite the law or use a form. Forward it immediately to the Co-ordinator, recording its exact terms and receipt date. Requests embedded in emails, complaints or grievances must be recognised separately. The school will help people clarify what they need without requiring them to justify the request.

The Co-ordinators log the request, appoints a lead, obtains DPO advice as needed and establishes a deadline and search plan. Only seek identity evidence where there are reasonable doubts, using a proportionate method. Verify a representative's authority. Check the child or adult learner considerations in section 7. Do not routinely demand identification from someone already known to the school.

11 2 Timing and clarification

Respond without undue delay and normally within one calendar month. The applicable period runs from receipt or, where lawfully required, receipt of necessary identity information or a permitted fee. Confirm representative authority promptly. A further two months is available only where necessary because of the complexity or number of the individual's requests; notify the person within the initial month and explain why. School holidays and staffing pressures are not grounds for extension.

For subject access only, where further information is reasonably needed to identify the information or processing activities requested, seek it promptly and explain why. The statutory clock can pause from the day clarification is sought through the day it is received. Record and communicate the revised deadline. This does not permit routine demands to narrow a clear request or pauses merely to agree response format. Other rights requests are not subject to this clarification pause.

Calculate a month using the corresponding date in the following month, or its last day where there is no corresponding date. If the deadline is a weekend or public holiday, use the next

working day. Record any legitimate adjustment or extension and arrange holiday cover. Keep the requester informed and continue work that can reasonably proceed.

11 3 Reasonable and proportionate searches

The school must make reasonable and proportionate searches. Search relevant school systems, email, structured paper files, therapy and safeguarding records, archives, recordings and processor-held information. Include school information held on staff devices or messaging services where there is reason to believe it exists. Consider name variants, relevant dates and custodians. Keep a record of systems, search terms, decisions and results.

Assess any proposed search limitation in the context of the request, the effort required and the importance of access. High volume or poor record management alone does not justify excluding information. The DPO must advise on any disputed limitation; explain the approach where appropriate and disclose information found through the remaining searches. Apply preservation arrangements promptly.

11 4 Reviewing and supplying information

Provide a copy of the person's personal data and the required supplementary information: purposes, categories, recipients, retention, source where relevant, rights, complaints routes, relevant automated decision information and international transfer safeguards. Supply it securely in an accessible form, normally a commonly used electronic format for an electronic request unless otherwise requested. The right is to personal data, not automatically to every unredacted document. [1, 6]

Review third-party information, confidentiality and applicable DPA exemptions individually. Consider whether third-party consent can be obtained or disclosure without consent is reasonable, taking account of all relevant circumstances. Use redaction where it permits disclosure. Safeguarding or therapy content is not automatically exempt; relevant serious-harm and other specific exemptions need a supported assessment and, where required, appropriate professional advice. Legal privilege and confidential reference exemptions also require proper analysis. [9]

The request lead and an appropriate second reviewer must check completeness, redactions, attachments and recipient details before release. The DPO must advise on refusals, exemptions and proposed fees. Access is normally free; a reasonable fee or refusal is permissible only on an established statutory ground, such as a manifestly unfounded or excessive request. Explain any refusal or charge, and the rights to complain and seek a judicial remedy, within the applicable deadline.

The child's UK GDPR access right must be distinguished from a parent's separate education-record right. In England, the statutory parental access regime for maintained schools does not generally extend to independent schools. Do not apply its 15-school-day rule to a UK GDPR request at Blossom House. Consider any separate legal or contractual entitlement on its own terms.

11 5 Other individual rights

The Co-ordinators must assess each right under its applicable conditions and explain the outcome. Rights do not all apply to every lawful basis or record. The school must consider:

- Rectification: correct inaccurate information and complete incomplete information where appropriate; assess disputed accuracy and restrict processing when required while checking it.

- Erasure: delete where the statutory conditions apply, while assessing exceptions such as a legal obligation, relevant public task or legal claims. Do not promise automatic deletion of necessary safeguarding or other protected records.
- Restriction: mark and isolate information so that prohibited uses stop, preserve it where required and tell the person before lifting a restriction.
- Portability: where applicable to automated processing based on consent or contract, provide the information the person supplied in a structured, commonly used, machine-readable format and transmit directly where technically feasible.
- Objection: assess objections to public tasks, recognised legitimate-interest or ordinary legitimate-interest processing. Stop unless compelling overriding grounds or the need for legal claims are established. Direct marketing objections must be honoured without a balancing test. Bring the right to object clearly and separately to the person's attention at first communication.
- Withdrawal of consent and automated decision safeguards: follow sections 5 and 16 and provide a practical route to exercise these protections.

Where required, inform recipients of rectification, erasure or restriction unless this is impossible or involves disproportionate effort, and identify those recipients to the person on request. Keep evidence of the actions and reasons. Requests for access to transfer safeguards must also be handled appropriately.

12 Data protection complaints

Anyone may complain about the school's use of their personal information. They may contact the DPO, write to the school marked for the Data Protection Co-ordinator, use the published school email route, or raise the concern verbally with staff. The school will provide an accessible electronic route and reasonable support; no mandatory form or legal wording is required. [CONFIRM A5: publish the monitored email or form and deputies.] All personnel must forward complaints immediately. The Co-ordinators log the complaint and appoints an appropriate investigator, avoiding conflicts of interest. A complaint involving the usual handler must go to an alternative senior lead with DPO advice. Keep safeguarding action, breach response and rights requests moving under their own requirements.

The school must acknowledge receipt within 30 days. The period begins the day after receipt; if its last day is a weekend or public holiday, the deadline moves to the next working day. Holiday cover must be maintained. Investigation begins promptly on receipt, not at the end of the acknowledgement period. [11]

Without undue delay, make appropriate enquiries, keep the person informed and communicate the outcome. Explain the findings, reasons, any remedial action and further complaint options. There is no general statutory rule requiring every investigation to be completed within 30 days; that is the acknowledgement deadline. An internal target may be set but must not justify unnecessary delay. [2, 11]

The complaints register must record receipt, acknowledgement, enquiries, updates, outcome, remedies and lessons. The Committee must address recurring concerns. People may complain to the ICO through ico.org.uk/make-a-complaint or telephone 0303 123 1113, and may seek judicial remedies. The school should have an opportunity to resolve concerns, but internal school complaint stages must not be presented as removing statutory rights or suspending other deadlines.

13 Sharing information and using suppliers

13 1 Sharing with other organisations

Before routine sharing, the responsible lead must identify the purpose, lawful basis, required information, recipient, security and retention arrangements, and what people need to be told. Verify recipients and authority, especially for telephone enquiries and requests from a new address. Share only what is necessary. Record significant disclosures and decisions. Local authorities, other schools, health professionals, therapists, safeguarding partners and regulators may be separate controllers rather than processors. Agree documented sharing arrangements for regular exchanges, covering roles, purpose, lawful bases, rights, security, incident handling and retention. Where parties jointly determine purposes and means, agree the Article 26 allocation and make its essence available to individuals.

A request from police, a local authority or another agency is not automatically a legal duty to disclose. Check the authority, necessity and any applicable exemption, obtaining DPO or legal advice where needed. This must not delay urgent safeguarding action under section 7. Internal access across departments or sites remains limited by work-related need; group membership alone does not justify sharing.

13 2 Processors and procurement

Before any supplier receives personal information, the service owner must determine its actual role and complete proportionate due diligence with IT and DPO input. Assess security, confidentiality, access, data locations, overseas support, sub-processors, retention, deletion, incident support, rights assistance and any use for the supplier's own purposes. This includes cloud, learning platforms, therapy tools, payroll, communications, storage and AI services.

Where the supplier is a processor, a binding Article 28 contract must define the processing, duration, nature and purpose, data types, data subject categories, and the school's rights and obligations. It must cover documented instructions, confidentiality, security, approved sub-processors and equivalent obligations, assistance with rights, breaches and DPIAs, return or deletion at contract end, audit information and notification of unlawful instructions.

Do not accept a supplier's claim of being "GDPR compliant" as sufficient evidence. Record approval before use, monitor material changes, review performance and plan secure exit and retrieval. The supplier register must identify an owner and review date. No free trial or staff purchase bypasses these checks.

14 UK international transfers

The relevant framework is UK restricted transfers, including making information accessible to a separate organisation outside the UK. Cloud hosting, overseas support, sub-processors and onward transfers must be checked; a UK sales address or UK data centre does not resolve the whole assessment.

Before a restricted transfer, the service owner must obtain DPO advice and record an available route: applicable UK adequacy regulations; appropriate safeguards such as the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU standard contractual clauses; or a strictly applicable statutory exception. An EU adequacy decision or EU clauses alone do not automatically satisfy UK requirements.

For safeguards-based transfers, complete the required assessment, commonly called a transfer risk assessment, applying the statutory data protection test. Acting reasonably and proportionately, assess whether protection after transfer is not materially lower than under UK law, and adopt additional measures where needed. Verify the scope and continuing validity of

adequacy or other arrangements. Exceptions are not a routine substitute for a sustainable supplier transfer arrangement.

Maintain the assessment, agreements, destination and onward-transfer details in the supplier and processing records, explain relevant safeguards in privacy information and review changes. Do not proceed where adequate protection cannot be established. Personnel travelling abroad must follow the school's approved access and device arrangements.

15 Data protection by design and new technology

Build privacy into procurement, service design and changes from the outset. Use the minimum data and access by default, clear retention, secure settings and usable rights mechanisms. Complete and record a DPIA screening before new or materially changed processing, including pilots and integrations. Consult the DPO early, before a purchase or operational commitment. A full data protection impact assessment (DPIA) is mandatory where processing is likely to create a high risk to individuals, including relevant systematic significant automated decisions, large-scale special category processing and large-scale systematic monitoring of publicly accessible areas. Consider the ICO's mandatory list and risk factors, particularly vulnerable pupils, profiling, biometrics, data matching and innovative technology.

The school requires a full DPIA before pupil profiling or any proposed solely automated significant decision, and for AI or monitoring proposals involving identifiable pupil health, therapy or safeguarding information. Other proposals must follow a recorded risk-based screening; a DPIA is not a substitute for a lawful basis or necessary consent.

The assessment must describe purposes and data flows, examine necessity and alternatives, assess likelihood and severity of harm, identify controls and residual risk, and record consultation, DPO advice, accountable approval and review dates. Seek views from affected people or representatives where appropriate. If high residual risk cannot be reduced, consult the ICO before starting the processing. Reassess when the purpose, system, supplier or risk changes.

15 1 Artificial intelligence

Personnel must not enter identifiable or confidential school information into unapproved AI tools. Approval must address provider training and reuse of inputs and outputs, retention, access, transfers, security, rights, accuracy, bias and explainability. Removing names from a detailed pupil account may not make it anonymous. Use synthetic or genuinely anonymous information for early testing wherever practicable. AI outputs are assistance, not verified records or professional findings. A competent staff member must check accuracy, sources and suitability before use, correct unsupported claims and avoid discriminatory assumptions. Do not rely on generated text for safeguarding, therapy, admissions, exclusions or employment decisions without the responsible professional's meaningful judgement. Record material AI use where needed for transparency and audit. Approval must include monitoring, an owner and a route to stop unsafe use. Assess whether the Children's Code and the specific UK GDPR requirements for online services likely to be accessed by children apply to a proposed service, including suppliers. Where applicable, address children's needs and protections in design and due diligence. These rules must not be assumed to apply identically to every internal school system.

16 Automated decisions and profiling

A solely automated decision has no meaningful human involvement. It is significant if it has a legal or similarly significant effect. Profiling may inform such decisions but is not synonymous with them. The DUAA framework in Articles 22A to 22D replaces the former general Article 22 restriction; it still imposes safeguards and specific restrictions. [3, 17] As a school policy safeguard, significant decisions about admission, exclusion, educational or therapy provision, safeguarding and employment must involve meaningful human judgement. Staff must have the competence, information, authority and time to question and change the outcome. Merely endorsing a system recommendation is insufficient. This is a school rule and must not be described as a universal legal ban on automated decisions.

Any proposal to vary that school rule requires a formal policy decision, a DPIA and DPO advice before use. A lawful Article 6 basis and the Article 22C protections are essential: information about the decision and practical means to make representations, obtain human intervention and contest it. Provide meaningful information about the logic, significance and envisaged consequences where required.

A significant solely automated decision using special category data is permitted only under the restricted Article 22B routes: the decision is based entirely on processing to which the person explicitly consented; or the decision is necessary for a contract with the person or required or authorised by law, and Article 9(2)(g) applies. The relevant UK law and safeguards must support that substantial public interest condition. Sole reliance on another Article 9 condition is insufficient. No significant solely automated decision may rely wholly or partly on recognised legitimate interests under Article 6(1)(ea).

17 Communications marketing and online services

Distinguish essential school communications from promotional messages. Admissions publicity, fundraising and promotional newsletters may be direct marketing. Apply UK GDPR and PECR requirements, obtain valid consent where required and use an exception only after its specific conditions have been checked. Give a clear opt-out and stop direct marketing promptly on objection, retaining only a minimal suppression record where needed.

The school must not use pupil information for targeted marketing without a specific approved assessment of lawfulness, fairness and children's protections. Publicity choices must not affect access to education or support. Website cookies and similar technologies require a current assessment and suitable information and consent controls where required; analytics and embedded services must not be assumed exempt merely because a provider describes them that way.

18 Accountability training and review

The Co-ordinators maintain a record of processing activities supported by department leads. It must identify the controller and DPO, purposes, people and data categories, recipients, international transfers and safeguards, retention and security measures. Supporting records must include legal bases and special category conditions, data flows, legitimate-interest assessments, consent evidence, notices, DPIAs, suppliers, sharing agreements, requests, complaints, breaches, training and disposal evidence.

The school must maintain its ICO registration and pay the data protection fee where required. Personnel receive suitable induction training before unsupervised access, refresher training at least annually and further training when risks or duties change. Role-specific training is required for those handling requests, safeguarding, therapy, HR, procurement and incidents. Managers must record completion and address gaps.

The Committee will review compliance at its six-monthly meetings, including outstanding actions, incidents, request and complaint performance, supplier changes, DPIAs and training. IT must test recovery and relevant security controls; department leads must review access, accuracy and disposal. Significant risks and overdue remedial actions go to the Principal and approval authority, supported by independent DPO advice.

Review this policy at least annually and sooner after a material legal, organisational or technology change, a serious incident or a significant audit finding. Record approval and version changes, communicate material updates and withdraw superseded operational copies. Non-compliance may lead to proportionate disciplinary or contractual action under the relevant procedures; personnel are encouraged to raise concerns promptly.

Read this policy with the school's privacy notices, safeguarding and child protection policy, safeguarding vulnerable adults policy, retention schedule, acceptable use and IT security rules, online safety policy, incident response procedure, recruitment and HR procedures, complaints procedure and information sharing arrangements. [CONFIRM A7: align document names and locations.]

Operational contact directory

DPO details

Satswana Ltd, info@satswana.com, 01252 759177

Written correspondence: Data Protection Committee: Blossom House School, Station Road, Motspur Park, New Malden, KT3 6JJ

AllDataProtectionCommittee@blossomhouseschool.co.uk

Appendix A School confirmation and approval checklist

For relevant school leads. Complete this checklist before approval. Replace the [CONFIRM] fields and then remove or retain this appendix as an approval record separate from the published policy. These are factual confirmations and implementation checks, not reasons to postpone existing legal duties.

Ref	Confirmation required	Suggested owner
A1	Confirm the approving body and accountable senior lead. Insert approval and effective dates; confirm September 2027 review. Do not backdate adoption.	Principal and Proprietor
A2	Confirm the controller's exact legal name, registered address and ICO reference. Confirm whether all three sites and all listed provision operate under the same controller; amend scope or controller arrangements if needed.	Operations and administration
A3	Confirm Committee chair, current role titles, membership, deputies and site representation. Confirm the IT Supervisor holds the Co-ordinator role and has capacity and cover. Retain or formally amend the six-monthly meeting cycle.	Principal and Committee
A4	Confirm Satswana Ltd's DPO appointment, info@satswana.com and 01252 759177. Confirm urgent escalation and absence arrangements; do not substitute another address without verification.	Co-ordinators and DPO
A5	Insert a monitored public email or form for requests and complaints, internal incident contacts, out-of-hours route and deputies. Test cover through weekends and school holidays and publish accessible routes.	Administration and IT
A6	Approve and identify the retention schedule, owner and storage location. Validate pupil, therapy, safeguarding, HR and DBS periods, preservation holds, backups and destruction evidence.	Department leads and DPO
A7	Confirm supporting procedure names and locations, actual security controls, annual training and records. Update privacy notices and request, complaint and breach logs to match this policy.	Committee and IT
A8	Review safeguarding sharing against KCSIE 2026 and the information sharing duty commencing 30 September 2026. Confirm school applicability, local partner arrangements and file transfer procedure.	DSL and DPO

Ref	Confirmation required	Suggested owner
A9	Validate processing purposes and legal bases, special category and criminal offence conditions, and any appropriate policy document. Check therapy providers' professional confidentiality and controller roles.	DPO and department leads
A10	Review supplier register, Article 28 terms, international transfers and transfer assessments. Check actual hosting, support locations, sub-processors and supplier AI training or reuse.	IT and service owners
A11	Inventory AI, profiling, CCTV, filtering, monitoring, biometrics and recordings. Confirm DPIAs, notices, permissions, retention and the school rule on significant decisions with human involvement.	IT, DSL and Principal

Appendix B Legal and guidance references

References checked on 17 September 2026. The numbered references support the relevant policy sections. Use current legislation and final guidance; a consultation draft is not treated as law. The school-specific governance and scope are drawn from the supplied Data Protection Policy 2025/26.

1 UK GDPR as amended

Principles, legal bases, transparency, rights, accountability, security, transfers and automated decisions.

2 Data Protection Act 2018 as amended

Schedules 1 to 3 and section 164A, including sensitive information conditions, exemptions and complaints.

3 Data Use and Access Act 2025

Amends rather than replaces UK GDPR and DPA 2018. Relevant provisions include sections 70, 76, 78, 80, 83 and 103.

4 UK GDPR Article 6

Includes recognised legitimate interests and requirements for other legal bases.

5 UK GDPR Articles 13 and 14

Privacy information, including the right to complain to the controller.

6 ICO guidance on responding to subject access

Timing, identity, clarification, extensions and fees.

7 DUAA section 76 and UK GDPR Article 12A

Statutory time limits and the subject access clarification pause.

8 ICO guidance on finding requested information

Reasonable and proportionate searches, archives and information held in different locations.

9 ICO guidance on education information

Pupil access, parental educational-record rights and education exemptions. Read with the wider ICO right of access guidance.

10 ICO personal data breaches guide

Assessment, notification, communication and record keeping.

11 ICO data protection complaints guidance

Acknowledgement, appropriate enquiries, progress updates and outcomes without undue delay.

12 ICO controller and processor contract requirements

Mandatory contract terms under Article 28.

13 Department for Education Keeping Children Safe in Education

Use the 2026 edition and current school safeguarding procedures.

14 Department for Education information sharing guidance

Updated 10 September 2026 for the information sharing duty commencing on 30 September 2026.

15 ICO international transfer guidance

UK adequacy, safeguards, exceptions and the data protection test.

16 ICO guidance on when a DPIA is required

Read with the ICO DPIA guidance, Children's Code and relevant online-service requirements.

17 DUAA section 80 and UK GDPR Articles 22A to 22D

Current statutory restrictions and safeguards for significant solely automated decisions.

18 Department for Education data protection in schools

Practical supporting guidance; apply provisions relevant to the school's legal s