READING BLUE COAT

Data Protection Policy

1. Background and Purpose

This policy explains how Reading Blue Coat School ("the School") complies with its obligations under data protection legislation and how it safeguards the personal data of pupils, parents, staff, governors, alumni, contractors and other third party individuals ("data subjects").

The School recognises the importance of personal data and is committed to ensuring it is:

- processed lawfully, fairly and transparently and is
- protected against unauthorised access, loss or misuse; and

2. Scope

Data protection is an important legal compliance issue for Reading Blue Coat School ("RBC"). During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about data subjects (in a manner more fully detailed in the School's Privacy Notice). This data may be held electronically, on paper, or otherwise recorded. The School, as "data controller", is liable for the actions of its staff, Trustees and Governors in how they handle such data. All staff (and volunteers) are responsible for:

- processing personal data only in accordance with this policy and other school procedures.
- undertaking appropriate data protection training;
- promptly reporting any suspected data breach.

For staff, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy will happen from time to time, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other Schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

3. Legal Framework

The School complies with the following legislation and regulatory guidance:

- The UK version of the General Data Protection Regulation ("UK GDPR")

- The Data Protection Act 2018 ("DPA"). The DPA 2018 includes specific provisions of relevance to independent Schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.
- The Data (Use and Access) Act 2025 ("DUAA")
- The Privacy and Electronic Communications Regulations 2003 ("PECR")
- Guidance issued by the Information Commissioner's Office ("ICO")
- Sector specific advice for bodies such as the Independent Schools' Bursars Association ("ISBA")

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including Schools that handle personal information. The ICO is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

4. Definitions

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its Trustees and Governors) is the data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Data Protection Co-ordinator** – a senior, non teaching member of staff who has strategic oversight of data protection compliance, including:
    - Resourcing,
    - Contractual arrangements with data processors, and
    - Financial and operational risk
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or 'personal data') -** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

5. Role and Responsibilities

- The Governing Body has overall responsibility for ensuring the School's compliance with Data Protection Law.
- The School has appointed the Bursar as the Data Protection Co-ordinator. The Bursar is supported in this capacity by the Compliance and Procurement Manager and the IT Manager. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Co-ordinator.

6. The Principles

The School processes personal data in accordance with the following six UK GDPR principles.

These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner (Lawful, fair and transparent)
2. Collected for specific and explicit purposes and only for the purposes it was collected for (Purpose limitation);
3. Relevant and limited to what is necessary for the purposes it is processed (Data minimisation);
4. Accurate and kept up to date (Accuracy);
5. Kept for no longer than is necessary for the purposes for which it is processed (Storage limitation); and
6. Processed in a manner that ensures appropriate security of the personal data (Integrity and Security).
7. *Evidenced* as being processed in a lawful manner (Accountability). The School must be able to *demonstrate* that the processing is lawful. This involves, among other things:
    - keeping records of data processing activities, including by way of logs and policies (see section "Record Keeping" 7 below);
    - documenting significant decisions and assessments about how personal data is used (including via formal risk assessment documents called Data Protection Impact Assessments); and
    - keeping an audit trail regarding data protection and privacy matters, including for example when and how the School's Privacy Notice was updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom).

7. Lawful grounds for data processing

Under the UK GDPR (Article 6), there are several different lawful grounds for processing personal data:

- performance of a contract (e.g. parent contracts, employment);
- compliance with a legal obligation;
- legitimate interests of the School (balanced against individuals' rights);
- consent, where appropriate;
- protection of vital interests.

Consent

Given the relatively broad definition of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject), it is considered preferable for the School to rely on other lawful grounds where possible.

Legitimate interests

This is the most flexible basis for processing. However, it requires transparency and an assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Compliance with a legal obligation

Such obligations may include connections with employment, engagement of services and diversity.

Contractual necessity

For example to honour a contract with staff or parents, or the engagement of contractors;

Protection of vital interests

This constitutes a narrower set of grounds for processing special categories of personal data (such as medical and safeguarding) which includes explicit consent, emergencies, and specific public interest grounds. It is processed in accordance with Articles 9 and 10 UK GDPR.

8. Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the Data Protection Co-ordinator, or the Compliance and Procurement Manager if they believe that *any* personal data is inaccurate, untrue, or has been incorrectly recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, students and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or students, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

9. Data handling

All staff have a responsibility to handle the personal data which they come into contact fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Child Protection and Safeguarding Policy
- E-Safety, Digital Communications and Student Device Policy
- GDPR Retention Policy
- Lone Working Policy
- Privacy Notice
- Security, CCTV and Access Control Policy
- Staff Code of Conduct

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

10. Avoiding, mitigating and reporting data breaches

Any personal data breaches must be reported immediately to the Data Protection Co-ordinator or the Compliance and Procurement Manager. The breach will be assessed and contained and, where

legally required (or the risk impact is perceived as high), data controllers will notify the ICO and affected individuals within 72 hours.

The School must maintain a breach register, in line with ICO expectations.

If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

11. Data security

The School implements appropriate technical and organisational security measures, including:

Staff Training and Awareness

The School sets out clear expectations in the Staff Handbook and the policies referred to above (Section 9 – Data Handling) regarding acceptable use of systems and data. All staff are required to remain mindful of the data protection principles (see section 7 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes such as filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Data Protection Co-ordinator.

All staff must attend mandatory, annual data protection and information security training which will cover:

- Regular updates and guidance on emerging risks, including phishing, and
- Cyber security threats and the use of new technologies

Access controls and secure authentication

In line with the School's digital safety policies:

- Staff will only be given access to systems and data relevant / necessary for their role(s).
- Strong password policies must be in place and, where appropriate, multi-factor authentication should be used;
- There must be secure management of user accounts, including prompt removal or amendment when roles change or employment ceases.

Encryption and secure storage

No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headmaster or Bursar.

Where an authorised worker is permitted to take data offsite it will need to be stored securely and / or encrypted in transit and, where appropriate, at rest.

Use of personal email accounts for official School business is not permitted as is the use of unencrypted personal devices for official School business.

All servers containing sensitive personal data must be approved and protected by security software. These servers must be kept in a secure location, away from general office space.

Data should be regularly backed up in line with the Schools back-up procedure. Copies of personal information, on a physical storage device, must be physically destroyed when they are no longer needed in line with the School's Data Retention Policy. Memory sticks or similar must be rendered permanently unreadable.

Risk Management and Assurance

The IT Manager will conduct regular reviews and tests of security measures, including risk assessments and, where appropriate, Data Protection Impact Assessments (DPIAs);

Special consideration should be given to the management and oversight of third-party suppliers to ensure they meet required data security standards (see below);

The Data Protection Co-ordinator and Compliance and Procurement Manager will review and test the will business continuity and disaster recovery arrangements on an annual basis to ensure they are fit to protect data in the event of system failure or incident

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the Bursar in the first instance, and at as early a stage as possible.

12. Rights of Individuals

Individuals have certain specific rights under data protection law, including the right to:

- Access personal data

  This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with within statutory timescales and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Data Protection Co-ordinator as soon as possible. The School will conduct a reasonable and proportionate search as clarified in the DUAA 2025.

- Rectification

  This requires the School to correct the personal data held about a subject if it is inaccurate;

- Erasure

  A data subject can request that their personal data be erased, where applicable, in certain circumstances;

- Restriction or objection to processing

  A data subject has the right to request that the School restricts its data processing activities (in certain circumstances);

- Data Portability

  A data subject has the right to receive personal data held by the School, for the purpose of transmitting it in a commonly used format to another data controller; and

- Objection

  To a particular processing activity where the individual feels this has a disproportionate impact on them, due to their particular circumstances.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

Any request from an individual purporting to exercise one or more of their data protection rights (including an SAR) must be communicated to the Data Protection Co-ordinator as soon as possible.

13. Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. Please contact the Data Protection Co-ordinator for further information and clarity, if necessary. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

14. Data Complaints

In line with the DUAA 2025, the School maintains a clear internal data protection complaints process.
Complaints will be:

- acknowledged within **30 days**;
- investigated promptly;
- responded to without undue delay before referral to the ICO, if unresolved .

15. Data Protection Policy Statement for Staff

All staff at the School have a responsibility to protect the personal data of pupils, colleagues, parents and other members of the School community. The School requires all staff to:

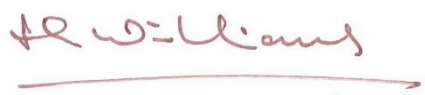
- act in accordance with this policy and all related data protection procedures at all times;
- only access and use personal data where it is necessary for their role and authorised by the School;
- handle all personal data securely and confidentially, whether in electronic or paper form;
- ensure that personal data is accurate, up to date and not disclosed inappropriately;
- follow School procedures when sharing personal data internally or externally;
- take all reasonable steps to prevent unauthorised access, loss or disclosure of personal data;
- immediately report any actual or suspected data breach to the Data Protection Co-ordinator;
- complete mandatory data protection and information security training and follow all guidance issued;

- comply with the School's policies on acceptable use of IT, remote working, use of personal devices and clear desk practices.

Failure to comply with this statement may result in disciplinary action and, where appropriate, legal consequences. The School will support staff by providing appropriate training, clear guidance and access to advice to ensure data protection obligations are understood and met.

These measures are regularly reviewed annually by the Bursar and Compliance and Procurement Manager to ensure ongoing effectiveness and alignment with current legal requirements and sector best practice.

Data protection law should not be seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Author(s):	Alexandra West (Bursar)
Date:	May 2026
Review Frequency:	Annually
Next Review Date:	May 2027
Agreed by:	 Howard Williams (Chair of Governors) *on behalf of the Full Governing Board*
Date of Agreement:	May 2026

Audit and Measurement Criteria		
Annually this privacy policy will be reviewed in line with updated legislation and revised as required.		
No	**Action**	**Frequency**
1	Review changes to UK GDPR and Data Protection Laws	Annually

Document Consultees	
Name	**Title**
Alexandra West	Bursar
Barry Hines	Head of IT

Associated/Linked/Related Documents			
Ref.	**Name**	**Type**	**Location/Link**
1	Privacy Notice	Policy	Privacy Notice December 2025.pdf
2	GDPR Retention Policy	Policy	GDPR Retention Policy March 2024.pd
3	Lone Working Policy	Policy	Lone Working Policy March 2024.pdf
4	E-Safety Policy	Policy	E-Safety Digital Communications and
5	Child Protection and Safeguarding Policy	Policy	Child Protection and Safeguarding Policy S

6	Data Use and Access Act (June 2025)	Law	**Data (Use and Access) Act 2025**
7	UK GDPR and the Data Protection Act 2018	Law	**Data protection: The UK's data protection legislation - GOV.UK**
5	Keeping Children Safe in Education	Law	**Keeping children safe in education 2025**
6	Data Complaints online form	Form	Upon Request from Bursar

Document History				
Version	**Updates**	**Owner**	**Author**	**Date**
1.	Original Policy	H Williams	T Tabrah	March 2024
2.	Annual amendment and review of policy in line with changes as per the DUAA (June 2025) and Data Protection Laws	H Williams	A West	May 2026