Boroughbridge High School and King James's School Federation

POLICY STATEMENT

Information Governance Policies

(GDPR)

Policies last reviewed (date) (Amendment only)	February 2026
Ratified by Governors (date)	February 2026
Next policy review due (date)	September 2026
Due for review by Governors (date)	September 2026
Staff Lead	Director of Business Services

MISSION STATEMENT:
This policy will support the school by being reflective of the Governors' direction and School's development plan. It will be used in an efficient and effective manner by ensuring that the Federation complies with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

Significant revisions since the last review:
- Addition of 'Reception' staff to CCTV access. (Page 44)

Contents

This policy is to ensure that the Federation complies with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation. In line with the requirements of the General Data Protection Regulation (GDPR), the Federation also has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were intended. This policy also has due regard to the following guidance, Information Records Management Society 'Information Management Toolkit for Schools'.

Data Protection Responsibilities

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

Each school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who has ultimate responsibility for operational risk, ensuring that the school's policies and procedures are effective and comply with legislation, and promoting good practice in school. In our organisation this role lies with the **Director of Business Services**.

Single Point of Contact (SPOC)

The SPOC is someone at school level who can take operational responsibility for data protection, including communicating with data subjects and the DPO. In our organisation this role lies with the **Network Manager.**

Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The Federation will ensure that IAO's are appointed based on sufficient seniority and level of responsibility. The Federation has responsibility for maintaining its records and record-keeping systems in line with statutory requirements. It is the responsibility of the Headteachers and Director of Business Services to ensure the policy is implemented correctly and in line with the policy. Employees of Boroughbridge High School and King James's School have a responsibility for the accuracy, safe handling, storage and disposal of records.

All staff

All staff, including governors or Trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school are responsible for collecting, storing and processing any personal data in accordance with this policy.

Data Protection Principles

We will comply with the data protection principles, as defined in Article 5 of the UK GDPR. We will ensure that personal information is:

- Processed lawfully, fairly and in a transparent manner **(Lawfulness, Fairness and Transparency).**
- Collected only for specified, explicit and legitimate purposes **(Purpose Limitation).**
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed **(Data Minimisation).**
- Accurate and where necessary kept up to date **(Accuracy).**
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed **(Storage Limitation).**
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage **(Security, Integrity and Confidentiality).**

We recognise that not only must we comply with the above principles, we must also demonstrate our compliance **(Accountability).**

Data Subject Rights

Under the UK GDPR, individuals have several rights in relation to the processing of their personal data:

Right to be informed
We provide individuals with privacy information at the time we collect their data, normally by means of a privacy notice, which is made easily accessible to the data subject. Privacy notices will be clear and transparent, regularly reviewed, and include all information required by data protection legislation.

Right of access
Individuals have the right to access and receive a copy of the information we hold about them. This is commonly known as a subject access request (SAR). We have in place a SAR procedure which details how we deal with these requests (Appendix Two).

Other rights include the right to rectification, right to erasure, right to restrict processing, right to object, right to data portability and rights related to automated decision-making, including profiling.

Requests exercising these rights can be made to any member of staff, but we encourage requests to be made in writing, wherever possible, and forwarded to [Phil Hemstock, hemstockp@king-james.co.uk who will acknowledge the request and respond within one calendar month. Advice regarding such requests will be sought from our DPO where necessary.

A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

Special Categories and conditions of processing

We process the following special categories (SC) of data:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation,
- biometric identifiers.

We also process criminal offence (CO) data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

We rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Article 9(2)(a) – explicit consent
We make sure that consent given by any person is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. We regularly review consents to ensure they remain up to date.

Examples of such processing includes when we use biometric (fingerprint) data for identification or authentication purposes for school meal payments; or when we ask for health or medical information from visitors to aid them in the event of an emergency.

Article 9(2)(b) – employment, social security or social protection
To comply with our legal requirements as an employer and safeguard our pupils, we need to collect some special category data.

Examples include when we carry out DBS checks on staff to evidence suitability for a role; collect medical information to put in reasonable adjustments at work and monitor staff absence; and keep records of an employee's trade union membership.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we rely on for this processing is Schedule 1, Part 1, (1) - employment, social security and social protection.

Article 9(2)(g) – reasons of substantial public interest
We have a wide variety of duties we must carry out in the public interest. Much of our processing of SC data is done so for the purposes of substantial public interest.

Examples include when we process SC data to identify students who require additional support such as special educational needs; processing safeguarding concerns to ensure the safety and wellbeing of pupils; or collecting medical information when monitoring pupil attendance or dietary requirements.

When processing data under Article 9(2)(g), we also require a Schedule 1 condition under the Data Protection Act 2018. The conditions we rely on for this processing are Schedule 1, Part 2, (6) – statutory and government purposes; (10) – preventing or detecting unlawful acts; and (18) – safeguarding of children and of individuals at risk.

Information Sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for us to share information with third parties. Routine and regular information sharing arrangements will be documented in our privacy notices and in our IAR.

Any further or ad-hoc sharing of information will only be done so in compliance with legislative requirements, including the ICO's data sharing code of practice. We will only share personal information where we have a lawful basis to do so, ensuring any disclosure is necessary and proportionate. All disclosures will be approved by the relevant staff member and recorded in a disclosure log.

Section 1: Document Protection & Retention Policy

1.Management of Trainee Teacher Records

1.1. Trainee Teacher records are specific documents that are prior to, during and after a trainee decides to apply and train with the Federation.

1.2. The information below is stored in a trainee file, and will be easily accessible:

- Attendance Information
- Additional support trainees may receive
- DBS
- Interview Records
- Major incidents notes
- Notes of complaints
- Trainee Progress Reports/Reviews/Grading
- UCAS Application Form

1.3. The following information is subject to shorter retention periods. These will be kept by the Teaching School Administrator in a separate file:

- Sick notes
- Correspondence with trainees, schools and HEIs about minor issues

1.4. Hard copies of disclosures relating to criminal records or serious incidents are retained by the HR team/designated lead and are stored in a secure office.

1.5. If a trainee enrolls on the course, the Federation will keep the trainee's records for 6 years.

2.Retention of trainee records and other trainee-related information

2.1. The table below illustrates the Federation's retention periods for individual trainee records and the action that will be taken after the retention period.

2.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Admissions		
UCAS application form	3 years after the date the entry was made	Information is reviewed and the register may be kept permanently
Interview Documentation	The current academic year, plus 1 year	Secure disposal
Identification Documents	Added to the pupil's record	Secure disposal
Qualifications Documents	Added to the pupil's record	Secure disposal
DBS Information	Until the appeals process has been completed	Secure disposal

Type of file	Retention period	Action taken after retention period ends
Pupil's Educational Records		
Trainee Progress Data	Deleted on completion of course	Secure disposal
Schools Placement Lists	Deleted on completion of course	Secure disposal
Trainee Review Documents	Deleted on completion of course	Secure disposal
Cause for Concern Documents	Deleted on completion of course	Secure disposal
Supplementary Information on Trainees	Deleted on completion of course	Secure disposal
Attendance		
Attendance registers	Deleted on completion of course	Secure disposal
Sick Notes/Leave of Absence Documents	Deleted on completion of course	Secure disposal
SEND		
Disability Documents	Deleted on completion of course	Secure disposal, unless it is subject to a legal hold

3. Educational Visits Outside the Classroom

3.1. The table below illustrates the Federation's retention periods for Educational Visits outside the Classroom and the action that will be taken after the retention period.

3.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Educational Visits outside the Classroom		
Records created to obtain approval to run Educational Visits outside the Classroom	Date of visit, plus 10 years	Secure disposal
Parental consent form from parent on trip with no major incident	Conclusion of trip	Secure disposal
Parental consent form from parent on trip with major incident	DOB of pupil plus 25 years	Secure disposal

4. Pupil's Educational Record

4.1. The table below illustrates the Federation's retention periods for Pupil' Educational Record and the action that will be taken after the retention period.

4.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Pupil's Educational Record		
Pupil's Educational Record required by the Education (Pupil Information) (England) Regulations 2005	DOB, plus 25 years	Secure disposal
Child protection information held on pupil file	Kept in sealed envelope and retained for the same period as pupil file	Secure disposal (shredded)
Child protection information held in separate files	DOB, plus 25 years	Secure disposal (shredded)
Attendance		
Attendance records	3 years from date the entry was made	Secure disposal
Authorised absence correspondence	Current year plus 2 years	Secure disposal
Special Educational Needs		
Special Educational Needs files, reviews and education plans	DOB plus 31 years	Secure disposal. This is a minimum retention period. SEN files can be retained for longer to respond to any claims against 'failure to provide sufficient education'. Any decision made to keep records beyond the minimum retention period must be documented.
Information and advice provided to parents regarding educational needs	DOB plus 31 years	Secure disposal
Accessibility strategy	DOB plus 25 years	Secure disposal

5. School Meal Management

5.1. The table below illustrates the Federation's retention periods for school meal management and the action that will be taken after the retention period.

5.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
School Meal Management		
Free School Meal register	Current year, plus 6 years	Secure disposal
School meal register	Current year, plus 3 years	Secure disposal
School meals summary sheets	Current year, plus 3 years	Secure disposal

6. Retention of staff records

6.1. The table below illustrates the Federation's retention periods for staff records and the action that will be taken after the retention period.

6.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Operational		
Staff personal file	Termination of employment, plus 6 years	Secure disposal
Timesheets	Current year, plus 6 years	Secure disposal
Annual appraisal and assessment records	Current academic year, plus 6 years	Secure disposal
Sickness Records	Current year, plus 6 years	Secure disposal
Annual leave	Current year, plus 2 years	Secure disposal
Unpaid leave / special leave records	Current year, plus 3 years	Secure disposal
Recruitment		
Records relating to new Headteacher appointment	Date of appointment, plus 6 years	Secure disposal
Records relating to new members of staff (unsuccessful candidates) appointment	Date of appointment of successful candidate, plus 6 months	Secure disposal
Records relating to new members of staff (successful candidates) appointment	Relevant information added to the member of staff's personal file. All other information retained for 6 months	Secure disposal
DBS checks	Up to 6 months	Secure disposal

Type of file	Retention period	Action taken after retention period ends
Proof of identify as part of the enhanced DBS check	After identity has been proven	Reviewed and a note kept of what was seen and what has been checked – if it is necessary to keep a copy this will be placed on the staff member's personal file, if not, secure disposal
Evidence of right to work in the UK	Added to staff personal file or, if kept separately, termination of employment, plus no longer than 2 years	Secure disposal
Disciplinary and grievance procedures		
Child protection allegations against a member of staff, including where the allegation is unproven	Until the individual's normal retirement age, or 10 years from the date of the allegation whichever is longer. Then review Malicious allegations are removed from personal files	Secure disposal
Oral warnings	6 months from date of warning	Secure disposal – if placed on staff personal file, removed from file
Written warning – level 1	6 months from date of warning	Secure disposal – if placed on staff personal file, removed from file
Written warning – level 2	12 months from date of warning	Secure disposal – if placed on staff personal file, removed from file
Final warning	18 months from date of warning	Secure disposal – if placed on staff personal file, removed from file
Records relating to no case to be answered	Dispose of at conclusion of the case, unless the incident is child protection related and is disposed of as above	Secure disposal

7. Retention of Teaching School Strategic Board Records

7.1. The table below illustrates the Federation's retention periods for senior Leadership and management records and the action that will be taken after the retention period.

7.2. All forms of information will be destroyed in line with the retention periods below.

File Description	Retention period	Actions taken at end of retention period
Governing Body		
Agendas for Governing Body board meetings	One copy is to be retained alongside the original set of minutes – all others to be disposed of	Secure disposal
Principal set of minutes, original and signed	Permanent	
Reports presented to the Governors	Minimum 6 years, if an individual is referred to these reports are kept permanently	Securely disposed of or, if they refer to individual reports, retained with the signed copy of minutes
Meeting papers relating to annual parents meeting held under the Education Act 2002, section 33.	Minimum of 6 years from date of meeting	Secure disposal
Instruments of Government, including Articles of Association	Permanent	Retention within school and offered to County Archives Service when school closes
Action plans created and administered by the Governing body	Duration of the action plan, plus 3 years	Secure disposal
Policy documents created and administered by the Governing Body	Until superseded	Secure disposal
Records that relate to complaints dealt with by the strategic board	Major complaints, current year plus 6 years. If negligence involved current year plus 15 years. If child protection or Safeguarding involved, current year plus 40 years	Secure disposal
Annual Reports created under the requirements of the Education (Governors Annual Reports)(England)(Amendments) Regulations 2002	3 years from date approved/declined	Secure disposal
Proposals concerning changing the teaching school status	Permanent	

File Description	Retention period	Actions taken at end of retention period
Teaching School Minutes and Documentation		
Minutes of teaching staff meetings and meetings of other internal administrative bodies	Date meeting, plus 3 years	Reviewed and secure disposal
Reports created by teaching staff	Date of report, plus minimum of 3 years	Reviewed and secure disposal
Records created by the Headteacher, Deputy Head or administrative team	Current academic year, plus 6 years	Reviewed and secure disposal
Correspondence created by the Headteacher, Deputy Head or administrative team	Date of correspondence, plus 3 years	Reviewed and secure disposal
School Development Plan	Duration of the plan, plus 3 years	Secure disposal

8. Retention of Health and Safety Records

8.1. The table below illustrates the Federation's retention periods for health and safety records and the action that will be taken after the retention period.

8.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Health and Safety		
Health and safety risk assessments	3 years plus duration of risk assessment	Secure disposal
Health and safety Policy	3 years plus life of policy	Secure disposal
Records relating to accidents and injuries at work	12 years from date of incident. 15 years is applied in the case of serious accidents	Secure disposal
Adults – accident reporting	6 years from date of the incident	Secure disposal
Pupils – accident reporting	Pupil's date of birth plus 25 years	Secure disposal
Control of Substances Hazardous to Health (COSHH)	Current year, plus 40 years	Secure disposal
Documentation relating to areas where employees and persons are likely to come into contact with asbestos	Date of last action, plus 40 years	Secure disposal

Type of file	Retention period	Action taken after retention period ends
Documentation relating to areas where employees and persons are likely to come into contact with radiation	Copy maintained until subject is aged 75. Record kept for minimum 30 years regardless	Secure disposal
Fire precautions log books	Current year, plus 3 years	Secure disposal

9. Retention of Financial Records

9.1. The table below illustrates the Federation's retention periods for financial records and the action that will be taken after the retention period.

9.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Payroll Pensions		
Maternity pay records	Current year, plus 3 years	Secure disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Current year, plus 6 years	Secure disposal
Risk management and insurance	Current academic year, plus 6 years	Secure disposal
Employer's liability insurance certificate	Closure of school plus 40 years	Secure disposal
Asset Management		
Burglary, theft and vandalism report forms	Current year, plus 6 years	Secure disposal
Inventory of furniture and equipment	Current year, plus 6 years	Secure disposal
Accounts and Statements including Budget Management		
Annual accounts	Current academic year, plus 6 years	Secure disposal
Loans and grants managed by the school	Date of last payment on the loan + 12 years then review	Secure disposal
All records relating to the creation and management of budgets	Current year, plus 3 years	Secure disposal
Student grant applications (Bursary/Foundation)	Current year, plus 3 years	Secure disposal
Invoices, receipts, order books, requisitions and delivery notices	Current financial year, plus 6 years	Secure disposal
Records relating to the collection and banking of monies	Current financial year, plus 6 years	Secure disposal

Type of file	Retention period	Action taken after retention period ends
Records relating to the identification and collection of debt	Current financial year, plus 6 years	Secure disposal
Contract Management		
All records relating to the management of contracts under seal	Last payment of contract, plus 12 years	Secure disposal
All records relating to the management of contracts under signature	Current academic year, plus 6 years	Secure disposal
All records relating to the monitoring of contracts	Current academic year, plus 6 years	Secure disposal
School Fund		
Cheque books, paying in books, ledgers, invoices, receipts, bank statements and journey books	Current academic year, plus 6 years	Secure disposal

10. Retention of other school records

10.1. The table below illustrates the Federation's retention periods for any other records and the action that will be taken after the retention period.

10.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Property Management		
Title deeds of properties belonging to the school	Permanent – follow the property unless the property has been registered with the Land Registry	Transferred to new owners if the building is leased or sold
Plans of property belonging to the school	Held for the period the building belongs to the school	Transferred to new owners if the building is leased or sold
Leases of property leased by or to the school	Expiry of lease, plus 6 years	Secure disposal
Records relating to the letting of school premises	Current financial year, plus 6 years	Secure disposal
Maintenance		
All maintenance records relating to the school carried out by contractors	Retained while the building belongs to the school	Secure disposal

Type of file	Retention period	Action taken after retention period ends
All maintenance records relating to the school carried out by school employees	Retained while the building belongs to the school	Secure disposal
Operational Administration		
Creation and publication of the school brochure and/or prospectus record	Current academic year, plus 3 years	Disposed of against common standards. A copy can be retained for archive purposes
Creation and distribution of circulars to staff, parents or pupils record	Current academic year, plus 1 year	Disposed of against common standards
Newsletters and other items with short operational use	Current academic year plus 1 year	Disposed of against common standards
Visitors' books and signing-in sheets	Current academic year plus 6 years	Reviewed then Secure disposal
Creation and management of Parent Teacher Associations and/or old pupil associations record	Current academic year, plus 6 years	Reviewed then Secure disposal

11. Statistics and Management Information

11.1. The table below illustrates the Federation's retention periods for Statistics and Management Information and the action that will be taken after the retention period.

11.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Statistics and Management Information		
Curriculum returns	Current year, plus 3 years	Secure disposal
Examination results	Current year, plus 6 years	Secure disposal
SATS results	Kept on student file until age 25 years. School may keep a composite record of all results for comparison purposes, current year plus 6 years.	Secure disposal
Examination papers	Kept until all appeals/validation processes are complete	Secure disposal
Published Admissions Number (PAN) Reports	Current year, plus 6 years	Secure disposal
Value Added and Contextual Data	Current year, plus 6 years	Secure disposal
Self-Evaluation Forms	Current year, plus 6 years	Secure disposal

12. Implementation of Curriculum

12.1. The table below illustrates the Federation's retention periods for Implementation of Curriculum and the action that will be taken after the retention period.

12.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Implementation of Curriculum		
Schemes of Work	Current year, plus 1 year	Review at end of each year and allocate further retention or secure disposal.
Timetable	Current year, plus 1 year	Review at end of each year and allocate further retention or secure disposal.
Class Records books	Current year, plus 1 year	Review at end of each year and allocate further retention or secure disposal.
Mark books	Current year, plus 1 year	Review at end of each year and allocate further retention or secure disposal.
Record of homework set	Current year, plus 1 year	Review at end of each year and allocate further retention or secure disposal.
Pupil's work	Return to pupil if possible, if not current year plus 1 year	Secure disposal

13. Local Authority

13.1. The table below illustrates the Federation's retention pertaining to the Local Authority and the action that will be taken after the retention period.

13.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Local Authority		
Secondary transfer sheets	Current year, plus 2 years	Secure disposal
Attendance returns	Current year, plus 1 year	Secure disposal
School Census returns	Current year, plus 5 years	Secure disposal
Circulars and other information sent from the Local Authority	Operational use	Secure disposal

14. Central Government

14.1. The table below illustrates the Federation's retention pertaining to the Central Government and the action that will be taken after the retention period.

14.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
Local Authority		
OFSTED reports and papers	Life of report, then review	Secure disposal
Returns made to central government	Current year, plus 6 years	Secure disposal
Circulars and other information sent from Central Government	Operational use	Secure disposal

15. Closed Circuit Television (CCTV)

15.1. The table below illustrates the Federation's retention pertaining to Closed Circuit Television recordings and the action that will be taken after the retention period.

15.2. All forms of information will be destroyed in line with the retention periods below.

Type of file	Retention period	Action taken after retention period ends
CCTV		
Digital recordings on HikVision IP based devices	8 days minimum unless recordings are required for the duration of an investigation	Secure deletion and over-write
Recordings made on Octar analogue recorders	1 month minimum unless recordings are required for the duration of an investigation	Secure deletion and over-write

16. Storing and Protecting Information

16.1. The Director of Business Services will undertake a risk analysis to identify which records are vital to school management and these records will be stored in the most secure manner. Back-ups are completed nightly and key data is secured in the cloud. Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access. Confidential paper records are not left unattended or in clear view when held in a location with general access. All staff members will implement a 'clear desk policy' to avoid unauthorised access to physical records containing sensitive or personal information. Any confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access. Visitors to areas of the school containing sensitive information are supervised at all times.

16.2 Staff are not permitted to use storage devices e.g. USB sticks to hold student data. Devices used by staff will be encrypted with a password. All electronic devices are password-protected to protect the information on the device in case of theft. All staff iPads are set up for remote detection, blocking or deletion of data in case of theft. Staff are provided with their own secure login and password.

16.3 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients. Any person taking the information from the school premises accepts full responsibility for the security of the data.

16.4 Emails should be kept for a maximum of two years before deletion. Records requiring a longer retention period, such as for legal or investigative purposes, should be archived to a user's secure storage area or printed paper copies should be kept.

16.5 Before sharing data, staff always ensure that:

- They have consent from data subjects to share it.
- Adequate security is in place to protect it.
- The data recipient has been outlined in a privacy notice.

16.6. The physical security of the schools' buildings and storage systems, and access to them, is reviewed termly by the Assistant Business Manager/Site Manager in conjunction with the Director of Business Services.

16.7. Any loss, damage or theft of data will be managed in accordance with the Federation's Information Security Policy. The Federation's takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

17. Information Audit

17.1. The schools conducts information audits to complete their Information Asset Registers on an annual basis against all information held by the schools to evaluate the information the schools are holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

- Paper documents and records
- Electronic documents and records
- Databases
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information

17.2. The information audit may be completed in a number of ways, including, but not limited to:

- Interviews with staff members with key responsibilities – to identify information and information flows, etc.
- Questionnaires to key staff members to identify information and information flows, etc.
- A mixture of the above

17.3. The designated DPO for each school is responsible for checking their Information Asset Register and will consult with staff members involved in the information audit process to ensure that the information is accurate.

18. Disposal of Data

18.1 Where disposal of information is outlined as standard disposal, this will be recycled appropriately to the form of the information, e.g. paper recycling, electronic recycling.

18.2. Where disposal of information is outlined as secure disposal, this will be disposed of by an approved Third Party securely and documented and electronic information will be scrubbed clean and, where possible, cut. The Information Asset Owner will keep a record of all files that have been destroyed. If, after the review, it is determined that the data should be disposed of, it will be destroyed in accordance with the disposal action outlined in this policy.

19. Monitoring and Review

19.1. This policy will be reviewed on an annual basis by the designated school DPO in conjunction with the Director of Business Services and the individual school's Headteacher. Any changes made to this policy will be communicated to all members of staff and the Federation Governing Body.

Section 2: Information Policy

This policy is to ensure that the Federation complies with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

1. Scope

The Information Policy applies to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

Information Security and Security Incident Reporting are addressed in separate policies.

2. Data Protection

Personal data will be processed in accordance with the requirements of GDPR and in compliance with the data protection principles specified in the legislation.

Each school has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025

The DPO is a statutory position and will operate in an advisory capacity. Duties will include:

- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;

- Facilitating a periodic review of the corporate information asset register and information governance policies;
- Assisting with the reporting and investigation of information security breaches
- Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
- Reporting to governors on the above matters

3. Information Asset Register

The DPO will advise the school in developing and maintaining an Information Asset Register (IAR). The register will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

The IAR will be reviewed annually and the Director of Business Services will inform the DPOs of any significant changes to their information assets as soon as possible.

4. Information Asset Owners

An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The school will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.

IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

5. Training

The Federation will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.

The DPOs will be consulted in relation to training where necessary; to ensure training resources and their implementation are effective.

The Federation will ensure that any third party contractors have adequately trained their staff in

information governance by carrying out the appropriate due diligence.

6. Privacy notices

Each school will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject. Our main privacy notice will be displayed on the schools websites in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of the year as part of their information pack. A privacy notice for employees will be provided at commencement of their employment with the school. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).

Privacy notices will be cleared by the Director of Business Services prior to being published or issued and aligned to DPO basic guidance. A record of privacy notices shall be kept on the schools' Information Asset Registers.

7. Information sharing

In order to efficiently fulfil our duty of education provision it is sometimes necessary for the school to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any ad hoc sharing of information will be done in compliance with our legislative requirements.

8. Data Protection Impact Assessments (DPIAs)

The Federation will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks.

The DPOs will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPOs will assist with the completion of the assessment, providing relevant advice.

9. Retention periods

Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition, IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

10. Destruction of records

Retention periods for records are recorded in the schools' IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins. Advice in regard to the secure destruction of electronic media will be sought from relevant IT support.

A record should be retained of all files destroyed including, where relevant:

- File reference number
- Description of file
- Date of disposal
- Method of disposal

- Officer who destroyed record

11. Third party Data Processors

All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.

Relevant senior leadership may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

12. Access to information

Requests for information under the Freedom of Information Act 2000 and Environmental Information Regulations 2004

Requests under this legislation should be made to admin@king-james.co.uk . The Head's PA and Director of Business Services is responsible for:

- Deciding whether the requested information is held;
- Locating, retrieving or extracting the information;
- Considering whether any exemption might apply and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

FOI requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.

Each request received will be acknowledged within 5 school days. The Chair of Governors and school's Headteacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:

- Document clearly the benefits of both disclosing or withholding the requested information; and
- Where necessary seek guidance from previous case law in deciding where the balance lies
- Consult the DPO

Reasons for disclosing or not disclosing will be reported to the next governing body meeting if applicable.

We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.

We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. Any charges will be formulated taking into account the limits set by the legislation.

We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 school days.

Requests for information under the GDPR - Subject Access Requests

Requests under this legislation should be made to admin@king-james.co.uk .

Any member of staff or governor may receive a request for an individual's personal information. Whilst GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the Head's PA and acknowledged within 5 days.

We must be satisfied as to your identity and may have to ask for additional information such as:

- Valid Photo ID (driver's license, passport etc);
- Proof of Address (Utility bill, council tax letter etc);
- further information for the school to be satisfied of the applicant's identity;

Only once the school is satisfied of the requestor's identity and has sufficient information on which to respond to the request will it be considered valid. We will then respond to your request within the statutory timescale of 30 calendar days.

The school can apply a discretionary extension of up to 60 calendar days to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first 30 days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.

Should we think any exemptions are necessary to apply we will seek guidance from a DPO to discuss their application.

If a subject access request is made by a parent whose child is 12 years of age or over we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information)(England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

13. Data Subject rights

As well as a right of access to information, data subjects have a series of other rights prescribed by the GDPR including:

- Right to rectification
- Right to erasure
- Right to restrict processing
- Rights in relation to automated decision making and profiling

All requests exercising these rights must be in writing and forwarded to admin@king-james.co.uk who will acknowledge the request and respond within 30 calendar days. Advice regarding such requests will be sought from a DPO.
A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

14. Complaints

Complaints in relation to FOI/EIR and Subject Access will be handled through our existing procedures. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the school's DPO on the address provided.

15. Copyright

The Federation will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the Federation is not re-used in a way which infringes those interests, whether or not any such warning has been given.

16. General

The Director of Business Services and Federation Governing Body will be responsible for evaluating and reviewing this policy.

Section 3: Information Security Policy

1. Introduction

As part of the Federation's programme to comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) it has written a new suite of Information Governance policies.

The Information Security Policy outlines the Federation's organisational security processes and standards. The policy is based upon the sixth principle of the GDPR which states organisations must protect the personal data, which it processes, against unauthorised loss by implementing appropriate technical and organisational measures. This policy has been written using the security framework recommended by ISO: 27000:1 (internationally recognised information Security standard).

This policy should be read in conjunction with the other policies in the Federation's Information Governance policy framework with particular focus on the Acceptable Use Policy Agreement and the Information Security Incident Reporting Policy.

2. Scope

All policies in the Information Governance policy framework apply to all Federation employees, any authorised agents working on behalf of the Federation, including temporary or agency employees, and third party contractors.

Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Speech, voice recordings and verbal communications, including voicemail,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

3. Access Control

The Federation will maintain control over access to the personal data that it processes.

These controls will differ depending on the format of the data and the status of the individual accessing the data.

The Federation will maintain an audit log detailing which individuals have access to which systems (both electronic and manual). This log will be maintained by the Director of Business Services.

4. Manual Filing Systems

Access to manual filing systems (i.e. non-electronic systems) will be controlled by a key management system. All files, that contain personal data, will be locked away in lockable storage units, such as a filing cabinet or a document safe, when not in use. Lockable storage units will be in relevant areas around the school. Current student documents will be in Learning Managers offices, former students will be stored in the Archive room. Finance documents will be stored in the Finance Archive room and HR will maintain their own locked area.

Keys to storage units will be locked in a pin-operated key safe. The Heads P.A. will be responsible for giving individuals access to the key safe. Access will only be given to individuals who require it to carry out legitimate business functions. The pin to the key safe will be changed on a regular basis or whenever a member of staff with the combination leaves the organisation.

5. Electronic Systems

Access to electronic systems will be controlled through a system of user authentication. Individuals will be given access to electronic filing systems if required to carry out legitimate functions. A two-tier authentication system will be implemented across all electronic systems. The two tiers will be user and unique Password.

Individuals will be required to change their password after an appropriate length of time so as to reduce risks of passwords being written down. Usernames will be suspended either when an individual is on long term absence or when an individual leaves employment of the School.

6. Software and Systems Audit Logs

The Federation will ensure that all software and systems have inbuilt audit logs so that the schools can ensure they can monitor what employees and users have accessed and what changes may have been made. Although this is not a preventative measure it does ensure that the integrity of the data can be assured and also deters individuals from accessing records without authorisation.

7. Data Shielding

The Federation does not allow employees to access the personal data of family members or close friends, except for those staff with children at the school who are required to do so as part of their job role. Employees should declare, upon employment, whether they are aware of any family members or friends who are registered at the schools.

The Federation will then keep paper files in a separate filing cabinet (with access restricted to minimal employees) and any electronic files will be locked down so that the declaring employee cannot access that data.

Employees who knowingly do not declare family and friends registered at the School may face disciplinary proceedings and may be charged with an offence under Section 170 of the Data Protection Act 2018 (unauthorised access to information).

8. External Access

On occasions the schools will need to allow individuals, who are not employees of their school, to have access to data systems. This could be, for example, for audit purposes, to fulfil an inspection, when agency staff have been brought in, or because of the Federation partnership. Each Headteacher is required to authorise all instances of third parties having access to systems. If the above individual is not available to authorise access then access can also be authorised by the Director of Business Services. Access to electronic data systems will require the additional authorisation of a Network Manager.

An access log, detailing who has been given access to what systems and who authorised the access, will be maintained by each school.

9. Physical Security

The Federation will maintain high standards of physical security to prevent unauthorised access to personal data. The following controls will be maintained across the Federation:

10. Clear Desk Policy

Individuals will not leave personal data on desks, or any other working areas, unattended and will use the lockable storage units provided to secure personal data when not in use. Individuals must also ensure they lock their computers when leaving their desk unattended.

11. Alarm System

The Federation will maintain security alarm systems at its premises so that, when the premises are not occupied, an adequate level of security is still in operation.

12. Building Access

External doors to the premises will be locked when the premises are not occupied. Only authorised employees will be key holders for the building premises. The Assistant Business Manager/Site Manager will be responsible for authorising key distribution and will maintain a log of key holders.

13. Internal Access

Internal areas, which are off limits to pupils and parents, will be kept locked and only accessed through pin numbers or keys. Pin numbers will be changed every six months or whenever a member of staff leaves the organisation. Keys will be kept in a pin-operated key safe.

14. Visitor Control

Visitors to the schools will be required to sign in via an electronic visitor register and state their name, organisation, car registration (if applicable) and nature of business. Visitors will be escorted throughout the School and will not be allowed to access restricted areas without employee supervision.

The visitor's register is stored electronically in an encrypted database for the duration of the current academic year. After which the data is securely deleted.

15. Environmental Security

As well as maintaining high standards of physical security, to protect against unauthorised access to personal data, the Federation must also protect data against environmental and natural hazards such as power loss, fire, and floods.

It is accepted that these hazards may be beyond the control of Federation but the schools will implement the following mitigating controls:

16. Back Ups

The Federation will back up their electronic data and systems every evening. These backups will be kept off site in Cloud storage by an external provider. This arrangement will be governed by a data processing agreement. Should the schools' electronic systems be compromised by an environmental or natural hazard then the schools will be able to reinstate the data from the backup with minimal destruction.

17. Fireproof Cabinets

The Federation will aim to only purchase lockable data storage cabinets that can withstand exposure to fires for a short period of time. This will protect paper records, held in the cabinets, from any minor fires that break out on the building premises.

18. Fire Doors

Areas of the premises which contain paper records or core electronic equipment, such as server boxes, will be fitted with fire doors so that data contained within those areas will be protected, for a period of time,

against any fires that break out on the premises. Fire doors must not be propped open unless automatic door releases are installed.

19. Fire Alarm System

The Federation will maintain a fire alarm system at its premises to alert individuals of potential fires and so the necessary fire protocols can be followed.

20. Systems Security

As well as physical security the Federation also protects against hazards to its schools' IT network and electronic systems. It is recognised that the loss of, or damage to, IT systems could affect the schools' ability to operate and could potentially endanger the lives of its pupils.

The Federation will implement the following systems security controls in order to mitigate risks to electronic systems:

21. Software Download Restrictions

Employees must request authorisation from a Network Manager before downloading software on to the schools' IT systems. The school's Network Manager will vet software to confirm its security certificate and ensure the software is not malicious. The school's Network Manager will retain a list of trusted software so that this can be downloaded on to individual desktops without disruption.

22. Phishing Emails

In order to avoid the schools computer systems from being compromised through phishing emails - employees are encouraged not to click on links that have been sent to them in emails when the source of that email is unverified. Employees will also take care when clicking on links from trusted sources in case those email accounts have been compromised. Employees will check with the school's Network Manager if they are unsure about the validity of an email.

23. Firewalls and Anti-Virus Software

The Federation will ensure that the firewalls and anti-virus software is installed on electronic devices and routers. The Federation will update the firewalls and anti-virus software when updates are made available and when advised to do so by the school's Network Manager. The Federation will review its firewalls and anti-virus software on an annual basis and decide if they are still fit for purpose.

24. Cloud Computing

The Federation utilises Microsoft OneDrive for Business as part of its Office 365 subscription. The storage should only be used for non-sensitive information where possible. Due to its encrypted access nature, some sensitive information can be stored for multi-user collaboration. Any information that is shared to an external email account should have the receivers email address specifically mentioned in the sharing permission link to ensure a verification email code is also sent to validate identity. Other forms of Cloud Storage should not be used for school purposes unless authorised first by the school's Network Manager.

25. Shared Drives

The schools maintain shared drives on their servers. Whilst employees are encouraged not to store personal data on the shared drive it is recognised that on occasion there will be a genuine business requirement to do so.

The shared drives will have restricted areas that only authorised employees can access. For example, a HR folder in the shared drive will only be accessible to employees responsible for HR matters. The school's

Network Manager will be responsible for giving shared drive access rights to employees. Shared drives will still be subject to the Federation's retention schedule.

26. Communications Security

The transmission of personal data is a key business need and, when operated securely is a benefit to the Federation and pupils alike. However, data transmission is extremely susceptible to unauthorised and/or malicious loss or corruption. The Federation has implemented the following transmission security controls to mitigate these risks:

27. Sending Personal Data by post

When sending personal data, excluding special category data, by post the School will use Royal Mail's standard postal service. Mail will be franked using the schools franking machine, authorised by Royal Mail. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject.

28. Sending Special Category Data by post

When sending special category data by post the schools will use Royal Mail's 1st Class Recorded postal service. Employees will double check addresses before sending and will ensure that the sending envelope does not contain any data which is not intended for the data subject. If the envelope contains information that is thought to be particularly sensitive then employees are advised to have the envelope double checked by a colleague.

29. Sending Personal Data and Special Category Data by email

The schools will only send personal data and special category data by email if one or more of the following conditions are met:

- Both the sending and receiving email addresses are GCSX or GCX etc.
- Using a secure email transmission portal such as Egress or Office 365 encrypted email system.

Employees will always double check the recipient's email address to ensure that the email is being sent to the intended individual(s).

30. Exceptional Circumstances

In exceptional circumstance the schools may wish to hand deliver, or use a direct courier, to ensure safe transmission of personal data. This could be because the personal data is so sensitive usual transmission methods would not be considered secure or because the volume of the data that needs to be transmitted is too big for usual transmission methods.

31. Using the BCC function

When sending emails to a large number of recipients, such as a mail shot, or when it would not be appropriate for recipients to know each other's email addresses then Federation employees will utilise the Blind Copy (BCC) function.

32. Surveillance Security

The Federation operates CCTV at its premises.

Due to the sensitivity of information that could be collected as a result of this operation, the Federation has a separate policy which governs the use of CCTV. This policy has been written in accordance with the ICO's Surveillance Code of School.

33. Remote Working

It is understood that on some occasion employees of the Federation will need to work at home or away from their school premises. If this is the case then the employees will adhere to the following controls:

34. Secure storage

Employees must not keep personal data or school equipment unsupervised at home for extended periods of time (for example when the employee goes on holiday).

Employees must not keep personal data or School equipment in cars if unsupervised.

35. Private Working Area

Employees must not work with personal data in areas where other individuals could potentially view or even copy the personal data (for example on public transport).

Employees should also take care to ensure that other household members do not have access to personal data and do not use school equipment for their own personal use.

36. Trusted Wi-Fi Connections

Employees will only connect their devices to trusted Wi-Fi connections and will not use 'free public Wi-Fi' or 'Guest Wi-Fi'. This is because such connections are susceptible to malicious intrusion. This includes hotspots available in hotels and café's/restaurants. Other government or education establishments with filtered internet connections are permissible.

When using home Wi-Fi networks employees should ensure that they have appropriate anti-virus software and firewalls installed to safeguard against malicious intrusion. If in doubt employees should seek assistance from the school's Network Manager.

37. Encrypted Devices and Email Accounts

Employees will only use school issued encrypted devices to work on Personal Data or pre- encrypted devices which are first approved by the school's Network Manager.

Employees will not use personal email accounts to access or transmit personal data. Employees must only use school issued, or school authorised, email accounts.

38. Data Removal and Return

Employees will only take personal data away from school premises if this is required for a genuine business need. Employees will take care to limit the amount of data taken away from the premises.

Employees will ensure that all data is returned to school premises either for re-filing or for safe destruction. Employees will not destroy data away from the premises as safe destruction cannot be guaranteed.

Section 4: Information Security Incident Reporting Policy

1. Introduction

This policy has been written to inform Federation employees what to do if they discover an information security incident.

Queries about any aspect of Boroughbridge High School's or King James's School's Information Governance strategy or corresponding policies should be directed to the school's Data Protection Officer at SchoolsDPO@veritau.co.uk.

2. Scope

This policy applies to all Federation employees, any authorised agents working on behalf of the Federation, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

They apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
- Speech, voice recordings and verbal communications, including voicemail;
- Published web content, for example intranet and internet;
- Photographs and other digital images.

3. Notification and Containment

Article 33 of the GDPR compels data controllers to report breaches of personal data to the Information Commissioner's Officer within 72 hours of discovery, if the incident is likely to result in a risk to the rights and freedoms of data subjects. Therefore it is vital that the Federation has a robust system in place to manage, contain, and report such incidents.

4. Immediate Actions (Within 24 Hours)

If an employee, governor, or contractor is made aware of an actual data breach, or an information security event (a 'near-miss'), they must report it to their line manager and the Director of Business Services within 24 hours. If the Director of Business Services is not at work at the time of the notification then their Out of Office email will nominate another individual to start the investigation process.

If appropriate, the officer who located the breach, or their line manager, will make every effort to retrieve the information and/or ensure recipient parties do not possess a copy of the information.

a) Assigning Investigation (Within 48 Hours)

Once received, the Director of Business Services will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings are:

Very Low/Low Risk

These do not need reporting to Veritau, but you should ensure you still complete the Data Breach Form and matrix and, record the incident on your Data Breach Log for internal reference.

This will ensure that key details around how and why the incident occurred, and what steps need to be taken to prevent similar breaches happening again, are considered and recorded by the school.

Moderate/High/Very High Risk

Contact the SchoolsDPO team at Veritau to report the incident to us as soon as possible. Once informed, we can advise you on the matrix and investigation, help you identify actions you need to take to control the breach, and measures you should put in place to prevent reoccurrence.

We will also assess and advise whether the breach needs reporting to the Information Commissioner's Office (ICO) within the statutory 72-hour deadline. If in doubt, please call us for advice.

The Director of Business Services will notify the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner (IAO) that the breach has taken place. The Director of Business Services will recommend immediate actions that need to take place to contain the incident.

The IAO will assign an officer to investigate white, green and amber incidents. Red incidents will be investigated by the school's Data Protection Officer with the assistance of Internal Audit and Counter Fraud Teams.

The severity rating is obtained by completing the Veritau Risk Matrix. This matrix is designed to help assess the risk associated with a data breach. Following a breach, complete the steps below by ticking the boxes that apply.

The risk score and rating should be provided to Veritau when you report the breach. The Risk Matrix is shown below:

Risk Matrix

Step 1

How many individuals' personal information is at risk?	Number of data subjects affected	Score	Selection
	0-10	+0	☐
	11 -50	+1	☐
	51-100	+2	☐
	101 -500	+3	☐
	500 -1000	+4	☐
	1000 or more	+5	☐

Step 2

Sensitivity factors – select each that apply		Score	Selection
Low	Contained no sensitive or confidential personal data.	-1	☐
	The information is already easily accessible or in the public domain, or it would have been published or released under FOI anyway.	-1	☐
	The information is encrypted, and it is therefore unlikely to be viewed.	-1	☐
	It was only disclosed internally, to a trusted professional who is bound by a code of confidentiality and has no personal relationship with the data subject.	-2	☐
	It was disclosed to an external trusted professional (e.g. a doctor or social worker) who is bound by a code of confidentiality and has no personal relationship with the data subject.	-1	☐
	Individuals identified are in different geographical locations or are unlikely to be known to each other and/or the recipient of the data.	-1	☐
	The information is unlikely to actually identify any individual(s).	-1	☐
High	Breach involves detailed profile information, e.g. work/school performance, salaries or personal life including social media activity, even if no special category data is involved.	+1	☐
	Breach involves high risk confidential or special category information e.g. SEND case or safeguarding notes, spreadsheets of marks or grades obtained, information about individual student discipline or sensitive disclosures, staff health information.	+1	☐
	The individuals affected are already known to be vulnerable, e.g. victims of a harassment or crime, a child, or family under social service support.	+1	☐
	The individuals affected are likely to be placed at risk of physical harm.	+1	☐
	Wider consequences are envisaged, e.g. embarrassment to the individual, reputational damage or similar effects. They	+1	☐

Sensitivity factors – select each that apply		Score	Selection
	may withdraw from engaging with the school and other professionals.		
	The incident is likely to attract media interest and/or a complaint has been made directly by a member of the public, another organisation or external individual.	+1	☐
	The incident is due to a failure to implement, enforce or follow appropriate organisational or technical safeguards to protect the information.	+1	☐
	There have been one or more previous incidents of a similar type in the last 12 months.	+1	☐
	The breach was a result of targeted malicious/criminal activity such as physical theft or a cyber attack.	+2	☐

Step 3

Effect of the breach on individuals (select one)		Score	Selection
No negative effects	There is absolute certainty that no negative effects will arise from the breach.	+0	☐
Low	Individuals are unaffected or may experience a few inconveniencies, which they will overcome easily (e.g. time spent re-entering information/changing passwords, annoyances or irritations).	+1	☐
Medium	Individuals may encounter inconveniences, which they will be able to overcome despite a few difficulties (e.g. inability to access business services, lack of understanding or stress).	+2	☐
High	Individuals may encounter significant consequences, which they should be able to overcome but with difficulties (e.g. recoverable or minor financial loss, property damage, factors affecting employment, health issues; risk of harassment, bullying or violence).	+3	☐
Very high	Individuals may encounter significant or even irreversible consequences, which they may not overcome (e.g. substantial debt or inability to work, loss of employment, long-term psychological or physical ill health, death or death threats).	+4	☐

Step 4

Likelihood that negative effects will occur (select one)			
Likelihood	**Description**	**Score**	**Selection**
Will not occur	There is absolute certainty of no negative effects. This rarely applies, and never applies to breaches involving vulnerable groups. If using this, provide evidence.	-2	☐
Not likely	There is a small possibility of a negative effect, but no evidence to rule out negative effects altogether.	+1	☐
Likely	It is fairly likely that a negative effect could occur as a result of the breach.	+2	☐
Highly likely	There is reasonable certainty that a negative effect will occur either shortly or at some point in the future.	+3	☐
Occurred	The negative effect arising from the breach has already occurred and is known.	+4	☐

Step 5

This step is only relevant if an individual has obtained, accessed, edited or destroyed data when they do not have authorisation to do so.
If this is step not relevant, please continue to the next section.

Actions and behaviour			
Factor	**Description**	**Score**	**Selection**
Intentional	The individual was not authorised to view the information but deliberately opened or searched for the data.	+3	☐
Accidental	The individual was not authorised to view the information, but accidentally opened the data in the course of their duties.	+1	☐
No pre-existing knowledge of or relationship	The individual does not know the data subject(s) via school or in their personal life.	+0	☐
Pre-existing knowledge of or relationship	The individual knows the data subject(s) either through school or in their personal life.	+2	☐

Step 6: risk scoring and rating

Please calculate the total from all the steps above, and record the risk score:

Risk Score	

Based on the score you calculated, use the table below to identify the risk rating for the incident.

Score	Risk Rating
< 2 (including < 0)	Very Low
3-5	Low
6-8	Moderate
9-10	High
11+	Very High

This risk rating should be provided to Veritau when reporting the breach.

Step 7: reporting to individuals and ICO
Below is a table of the suggested reporting requirements indicated for each risk rating.

Risk Rating	Mandatory to inform the data subjects*	Reportable to ICO
Very Low	No	No
Low	No	No
Moderate	No	No
High	No	Yes
Very High	Yes	Yes

*There can be other factors to consider when reporting to individuals. Please see the additional guidance document and refer to Veritau for advice.

b) Reporting to the ICO/Data Subjects (Within 72 Hours)

The SIRO, in conjunction with the service manager, Director of Business Services, IAO and DPO will make a decision as to whether the incident needs to be reported to the ICO, and also whether any data subjects need to be informed. The service manager/IAO will be responsible for liaising with data subjects and the DPO for liaising with the ICO.

c) Investigating and Concluding Incidents

The Director of Business Services will ensure that all investigations have identified all potential information risks and that remedial actions have been implemented.

When the DPO has investigated a data breach then the SIRO must sign off the investigation report and ensure recommendations are implemented across the Council.

The SIRO will ensure all investigations have been carried out thoroughly and all highlighted information security risks addressed.

Section 5: Parents and Pupils Privacy Notice

This Privacy Notice has been written to inform parents and pupils of King James's School and Boroughbridge High School (the 'Federation') about what we do with your personal information. This Notice may be subject to change.

Who are we?

The Boroughbridge High School and King James's School Federation is a 'Data Controller' as defined by Article 4 (7) of GDPR. This means that we determine the purposes for which, and the manner in which, your personal data is processed. We have a responsibility to you and your personal data and will only collect and use this in ways which are compliant with data protection legislation.

The Federation has appointed Veritau Ltd to be its Data Protection Officer (DPO). The role of the DPO is to ensure that the school is compliant with GDPR and to oversee data protection procedures. If you would like to discuss anything in this privacy notice, please contact (insert SPOC details) or Veritau Ltd. Veritau's contact details are:

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025

What information do we collect?

The categories of information that we collect, hold and share include the following:

- Personal information of pupils and their family members (e.g. name, pupil number, DOB and address)
- Educational and assessment attainment (such as KS1 and phonics results, post 16 courses and relevant results)
- Free school meal eligibility
- Attendance information (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Safeguarding information (including but not limited to court orders and professional involvement)
- Financial and grant information where applicable
- Photographs and communication preferences

We will also process certain 'special category' data about our pupils including:

- Relevant medical information - please be aware that where the pupil has a severe allergy or is thought to be at risk of needing emergency care for a medical issue then this will be shared with all relevant staff members. We may do this in the form of photo identification in the staff room to ensure that all staff members are aware of the issues should an emergency situation arise
- Special Educational Needs and Disabilities information (including the needs and ranking)
- Biometric data e.g. thumbprints

Why do we collect your personal data?

We use the information we collect:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to keep children safe (food allergies or emergency contact details)to meet the statutory duties placed upon us by the DfE

Any personal data that we process about our pupils and parents is done so in accordance with Article 6 and Article 9 of GDPR.

Our legal basis for processing your personal data, in line with Article 6(1)(c) (legal obligation) includes (but not necessarily limited to):

- Education Act 1944,1996, 2002, 2011
- Education and Adoption Act 2016
- Education (Information About Individual Pupils)(England) Regulations 2013
- Education (Pupil Information) (England) Regulations 2005
- Education and Skills Act 2008
- Children Act 1989, 2004
- Children and Families Act 2014
- Equality Act 2010
- Education (Special Educational Needs) Regulations 2001

We also process information in accordance with Article 6(e) (public task), Article 6(a) (consent), Article 9 (2)(a) (explicit consent where applicable) and Article 9(2)(g) (reasons of substantial public interest). Such as processing, which is not mandatory but is considered to be in our pupils' interests, including:

- School trips
- Extra-curricular activities
- Events and newsletters

We mainly collect pupil information through admission forms and common transfer file or secure file transfer from previous school. The majority of pupil information you provide to us is mandatory in line with your parental responsibility – for further details please see the following link https://www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility/understanding-and-dealing-with-issues-relating-to-parental-responsibility.

However, some information we ask for on a voluntary basis. When we do process this additional information we will ensure that we ask for your consent to process it.

Where we are processing your personal data with your consent you have the right to withdraw that consent. If you change your mind, or are unhappy with our use of your personal data, please let us know by contacting:

King James's School: admin@king-james.co.uk

Boroughbridge High School: schooladmin@boroughbridgehigh.com

Who do we obtain your information from?

Much of the information we process will be obtained directly from you (pupils and parents). We will also process information received from:

- Department for Education (DfE)
- North Yorkshire Educational Authority
- Previous schools attended

Who do we share your personal data with?

We routinely share pupil information with:

- schools that the pupils attend after leaving us
- institutions and employers
- awarding bodies
- North Yorkshire Educational Authority
- the Department for Education (DfE)
- the Education Funding Agency (EFA)
- National Health Service, social care and youth support services
- Police
- trusted third party data analysis providers
- trusted online revision and resource providers

For more information on information sharing with the DfE (including the National Pupil Database and Census) please go to: https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

We will not share any information about you outside the school without your consent unless we have a lawful basis for doing so. For example, we may also share your data with classroom/teaching apps and some website for the purpose of enhancing pupil learning. Where we do this we will rely on either Article 6(e) (public task) or Article 6(a) (consent).

Where we rely on Article 6(e) you have the right to object to processing and where we are relying on Article 6(a) you have the right to withdraw that consent at any time. Please see section below on data subject rights.

Once our pupils reach the age of 13, we also pass information to our Local Authority and / or provider of youth support services as stipulated under section 507B of the Education Act 1996. The information provided includes

addresses, DOB of pupil/parents, and any other information necessary for the provision of the service including gender or ethnicity.

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

For more information regarding services for young people please visit our Local Authority's website: https://www.northyorks.gov.uk/

How long do we keep your personal data for?

The Federation will keep your data in line with our Information Policy. Most of the information we process about you will be retained as determined by statutory obligations. Any personal information which we are not required by law to retain will only be kept for as long as is necessary to fulfil our organisational needs.

What rights do you have over your data?

Under GDPR parents and pupils have the following rights in relation to the processing of their personal data:

- to be informed about how we process your personal data. This notice fulfils this obligation
- to request access to your personal data that we hold, and be provided with a copy of it
- to request that your personal data is amended if inaccurate or incomplete
- to request that your personal data is erased where there is no compelling reason for its continued processing
- to request that the processing of your personal data is restricted
- to object to your personal data being processed

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact the school's DPO on the school's admin email address provided above.

Please be aware that usually pupils are considered to have the mental capacity to understand their own data protection rights from the age of 12 years old. A school may therefore consult with the pupil if it receives a request to exercise a data protection right from a parent.

If we cannot resolve your concerns you may also complain to the Information Commissioner's Office (the Data Protection Regulator) about the way in which the Federation has handled your personal data. You can do so by contacting:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
dataprotectionfee@ico.org.uk
Or via their live chat.
Opening Hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

Section 6: CCTV Policy (and Privacy Notice)

1. Rational

The purpose of this Policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) systems at King James's School and Boroughbridge High School, hereafter referred to as 'the Federation'. The Federation is fully committed to operating a safe environment for students, staff and visitors, as well as to protect school property.

The systems, owned by the Federation, comprise a number of fixed and dome cameras located around the school sites which may include sound functionality. All cameras are monitored within the schools and by the Federation's preferred monitoring company.

CCTV systems are based around digital technology and therefore need to be treated as information that will be processed in accordance with the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018. This document sets out the accepted use and management of the CCTV system and images to ensure the school complies with GDPR, Human Rights Act 1998 and other legislation. The Federation has produced this Policy in line with the Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

The Code of Practice will be subject to review periodically, but at least biannually, to include consultation as appropriate with interested parties.

The CCTV systems are owned by the Federation. Deployment of the systems is determined by the schools' leadership teams. All authorised operators and employees with access to images will be aware of the procedures and responsibilities that need to be followed.

2. Principles of CCTV

The objectives of the scheme are:

- To increase personal safety and reduce the fear of crime, intimidation and physical abuse
- To support the police in a bid to deter, detect and investigate crime
- To protect the school buildings and their assets to ensure they are kept free from intrusion, vandalism, damage or disruption
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the school
- To protect and maintain the wellbeing of young people and vulnerable adults who may be on the site
- Monitor security of buildings
- Identify vehicle movement
- Assist with the identification of actions/activities that might result in disciplinary proceedings against staff and students

3. Statement of Intent

The CCTV systems are registered with the Information Commissioner under the terms of GDPR and will seek to comply with the requirements both of GDPR and the Commissioner's Code of Practice.

CCTV warning signs will be clearly and prominently placed at all external entrances to the schools, including school gates. In areas where CCTV is used, the schools will ensure that there are prominent signs placed at

both the entrance of the CCTV zone and within the controlled area. The planning and design will endeavour to ensure that the scheme will give maximum effectiveness and efficiency. It is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage. The scheme will monitor activities within the schools and their car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the schools occupants, together with their visitors.

CCTV will not generally be used in classrooms but in areas within school that have been identified by staff and pupils as not being easily monitored. CCTV will only be used in classrooms where there is the need to monitor the security of equipment, such as I.T.

The Federation may in exceptional circumstances set up covert monitoring. If such surveillance is requested, for example, by the police for the detection and prevention of crime, specific legal requirements will have to be satisfied, mainly contained in the Regulation of Investigatory Powers Act.

Materials or knowledge secured as a result of the CCTV system will not be used for any commercial purpose. Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Downloads will never be released to the media for purposes of entertainment.

Static cameras are positioned to ensure that they do not focus on private homes, gardens and other areas of private property.

4. **E-Monitoring**

We operate e-safety monitoring software systems to:

- Safeguard our pupils and staff
- Promote wellbeing and early intervention
- Ensure appropriate use of school assets and resources
- Monitor compliance with school rules and policies

The school uses Impero.

5. **Call Recording**

We may record incoming and outgoing telephone calls:

- For quality monitoring and staff training purposes
- For efficient resolution of disputes and complaints
- To assist with informal or formal investigations, where appropriate
- As evidence of safeguarding concerns

The school uses the internal Panosonic phone system.

6. **System Operation**

The systems will be administered and managed by the school's Headteacher, in accordance with the principles and objectives expressed in the code.

The day-to-day management will be the responsibility of the Director of Business Services, assuming the role of the Data Controller.

The CCTV system will be operated 24 hours each day, every day of the year. Any changes to the CCTV system will be communicated via appropriate signage, visible in all areas of the school. Signage will include what software is being used, CCTV, Audio, or both. The signage will be clear and kept unobstructed, so that anyone entering the area will be aware that they are being recorded.

7. **Control Room**

Access to the CCTV facilities will be strictly limited to the leadership team, IT support team, pastoral team, Business Services Assistant, Reception staff, and Caretakers. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

The Federation will ensure that there is a consistent approach across all operating users to managing access to, and the storage of CCTV images.

All retained data will be stored securely.

Where data is to be released to the police, this will only be released to the police on receipt of a Data Request Form, kept with Business Services, and sight of their warrant card.

8. **Subject Access Requests**

Individuals have the right to request access to CCTV footage relating to themselves under GDPR. All requests should be made in writing to the school's Headteacher and include sufficient information to enable the footage relating to them to be identified (e.g. date, time and location). The Federation will respond to requests within 30 calendar days of receiving the written request. The school reserves the right to charge a fee of £10 to cover administration costs. The school reserves the right to refuse access to CCTV footage in line with the Information Commissioner's Office (ICO) CCTV Code of Practice.

For further information on security and privacy relating to CCTV, reference should be made to the Document Retention Policy.

9. **Access to and Disclosure of Images to Third Parties**

There will be no disclosure of recorded data to third parties other than to authorised personnel such as law enforcement agencies, prosecution agencies and Insurance companies (or legal representatives) where these would reasonably need access to the data (e.g. investigators). Requests should be made in writing to the school's Headteacher. The data may be used within the Federation's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

The details of any data released to a third party should be formally recorded, to also include the date of the disclosure, to whom, reasons for the request, information to identify the individual, proof of identity and any other relevant information, such as a crime incident number. If the Federation cannot comply with the request, the reasons will be documented.

Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under GDPR.

Prior to authorisation from the school's Headteacher, the requesting applicant must have demonstrated and documented that all reasonable procedures and practices were put in place to prevent suspected illegal or unauthorised activity from taking place.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom. The Federation's Legal Team may be involved. This decision will likely be taken under the following circumstances:

- informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording
- there is reasonable cause to suspect that illegal activity is taking place or is about to take place or unauthorised activity is taking place; that may seriously or substantially affect the operation or reputation of the Federation

10. **Complaints**

Complaints and enquiries about the operation of CCTV within school grounds should be directed to the school's Headteacher in the first instance. Any suspected breach of this Policy by school staff will be considered under the schools Disciplinary Policy and Procedures.

11. **Data Protection**

For the purpose of GDPR, Veritau is the Data Controller.

- CCTV digital images, if they show a recognisable person, are personal data and are covered by GDPR. This Policy is associated with the schools GDPR Policy, the provisions of which should be adhered to at all times
- The Federation has registered its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO)
- Where new cameras are to be installed on school premises, Part 4 of the ICO's CCTV Code of Practice will be followed before installation:

- the appropriateness of and reasons for using CCTV will be assessed and documented
- the purpose of the proposed CCTV system will be established and documented
- responsibility for day-to-day compliance with this Policy will be established and documented

Section 7: Privacy Notice - CCTV

This privacy notice has been written to inform alumni of The Boroughbridge High School and King James's School Federation about how and why we process your personal data when maintaining our relationship with you post-studies.

Who are we?

The Boroughbridge High School and King James's School Federation is a data controller as defined by the UK GDPR. This means that we determine the purposes for which your personal data is processed and the manner of the processing. We will only collect and use your personal data in ways that are compliant with data protection legislation.

The school has appointed Veritau Ltd as its Data Protection Officer (DPO). The role of the DPO is to monitor our compliance with the UK GDPR and the Data Protection Act 2018 and advise on data protection issues. If you would like to discuss this privacy notice or our use of your data, please contact Veritau or Phil Hemstock hemstockp@king-james.co.uk (SPOC).

Schools Data Protection Officer
Veritau
West Offices
Station Rise
York
North Yorkshire
YO1 6GA

schoolsDPO@veritau.co.uk // 01904 554025

What personal information do we collect?

The personal data we collect about you includes:

By using CCTV systems the Federation collects, stores, and uses static or moving images of individuals located in the surveillance area.
The Federation may be able to identify those individuals by using other existing information.

Why do we collect your personal information?

We process your information for the purposes outlined below:

- For the safeguarding of children
- For the prevention and detection of crime.

What is our lawful basis for processing your information?

Under the UK GDPR, it is essential to have a lawful basis when processing personal information. We normally rely on the following lawful bases:

- Article 6(1)(a) – consent
- 6(1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – Safeguarding children.
- 6(1)(f) - Processing is necessary for the purposes of legitimate interests - prevention and detection of crime.

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind about our use of your personal data, please let us know by contacting the SPOC, Phil Hemstock hemstockp@king-james.co.uk.

There may be occasions where our processing is not covered by one of the legal bases above. In that case, we may rely on Article 6(1)(f) - legitimate interests. We only rely on legitimate interests when we are using your data in ways you would reasonably expect.

Who do we obtain your information from?

We normally receive this information directly from you.

Who do we share your personal data with?

We will only share CCTV footage with other agencies where there is a lawful reason to do so - for example to share with the police for the purposes of crime prevention or to assist in locating an absconding pupil.

How long do we keep your personal data for?

We will retain your information in accordance with our Records Management Policy and Retention Schedule shown on page 12. The retention period for most of the information we process about you is determined by statutory obligations. Any personal information which we are not required by law to retain will only be kept for as long as is reasonably necessary to fulfil its purpose.

We may also retain some information for historical and archiving purposes in accordance with our Records Management policy.

The school will retain data for:

Digital recordings on HikVision IP based devices	8 days minimum unless recordings are required for the duration of an investigation
Recordings made on Octar analogue recorders	1 month minimum unless recordings are required for theduration of an investigation

International transfers of data

Although we are based in the UK, some of the digital information we hold may be stored on computer servers located outside the UK. Some of the IT applications we use may also transfer data outside the UK.

Normally your information will not be transferred outside the European Economic Area, which is deemed to have adequate data protection standards by the UK government. In the event that your information is transferred outside the EEA, we will take reasonable steps to ensure your data is protected and appropriate safeguards are in place.

What rights do you have over your data?

Under the UK GDPR, individuals have the following rights in relation to the processing of their personal data:

- to be informed about how we process your personal data. This notice fulfils this obligation.
- to request a copy of the personal data we hold about you.
- to request that your personal data is amended if inaccurate or incomplete.
- to request that your personal data is erased where there is no compelling reason for its continued processing.
- to request that the processing of your personal data is restricted.
- to object to your personal data being processed.

If you have any concerns about the way we have handled your personal data or would like any further information, then please contact our DPO using the details provided above.

If we cannot resolve your concerns then you may also complain to the Information Commissioner's Office, which is the UK's data protection regulator. Their contact details are below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

0303 123 1113
dataprotectionfee@ico.org.uk
Or via their live chat.

Opening Hours are Monday to Friday between 9am and 5pm (excluding bank holidays). You can also report, enquire, register and raise complaints with the ICO using their web form on Contact us | ICO.

We reserve the right to change this privacy notice at any time. We will normally notify you of changes that affect you. However, please check regularly to ensure you have the latest version.

This privacy notice was last reviewed March 2023.

Section 8: Biometrics Policy

1. Introduction

This Policy fulfils the Federations obligation to have an appropriate policy document in place where the processing of Special Category Biometric data is in place.

The Biometric Policy governs the Federation's collection and processing of biometric data. The nature of this processing, including what information is processed and for what purpose, is outlined in the School's privacy notices.

The Federation will comply with the additional requirements of sections 26 to 28 of the Protections of Freedoms Act 2012, this includes provisions which relate to the use of biometric data in schools and colleges who use an automated biometric recognition system. These provisions are in addition to the requirements of the UK GDPR.

This policy complements the School's existing records of processing required under Article 30 of the General Data Protection Regulation (The UK GDPR) 2018, which is fulfilled through the School's Information Asset Register. It should also be read in conjunction with the other policies and privacy notices in the School's Information Governance policy and privacy notice framework.

2. Scope

All policies in the Federation's Information Governance policy framework apply to all Federation employees, any authorised agents working on behalf of the Federation, including temporary or agency employees, and third party contractors. Individuals who are found to knowingly or recklessly infringe these policies may face disciplinary action.

The policies apply to information in all forms including, but not limited to:

- Hard copy or documents printed or written on paper,
- Information or data stored electronically, including scanned images,
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer,
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card,
- Information stored on portable computing devices including mobile phones, tablets, cameras and laptops,
- Published web content, for example intranet and internet,
- Photographs and other digital images.

3. Definition of "Biometric Data"

Biometric data is defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the

system to see if there is a match in order to recognise or identify the individual. For example, where a fingerprint is used to identify an individual and allow them access to an account.

Biometric Data is defined in the UK GDPR 2018 and the Data Protection Act 2018 as a special category of personal data, and it therefore requires additional measures to be put in place in order to process it, as detailed below.

4. Definition of "Processing"

'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

a) Recording pupils' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
b) Storing pupils' biometric information on a database system; or
c) Using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise pupils.

Any processing of Biometric data will only be carried out where there is a lawful purpose for the processing, as defined under Article 6 and Article 9 (Schedule 1) of the UK GDPR 2018. The purposes will be outlined in the Federation schools' privacy notices which will be made available to the relevant individuals.

5. What Counts as Valid Consent?

The Data Protection Act 2018 states that an individual can consent to the use of their own personal data when they are considered to have the adequate capacity to fully understand what they are consenting to. Most individuals are considered to reach this capacity over the age of 12, however where the Federation considers the individual to not have adequate capacity to consent themselves, the consent of one or more of their parents/carers will be sought.

The Federation will ensure that the member of staff, or the student and both of their parents/carers (if possible) will be informed of the Federation's intention to process the individual's biometric data. This will be carried out through readily available privacy notices and communications, prior to or at the point of obtaining consent, and will include:

- The type of biometric data
- What it will be used for
- The parent's and pupil's rights to withdraw or refuse consent
- What the alternative arrangement will be if consent is refused or withdrawn

Under no circumstances will the Federation collect or process the biometric data of an individual without their explicit consent or the consent of at least one authorised parent/carer, this will be obtained prior to obtaining any biometric data. If one parent objects in writing, then the Federation will not be permitted to take or use that child's biometric data.

All consent must be freely-given, specific, informed and unambiguous, and will be obtained through a clear affirmative action. The Federation will collect consent by letters home and online forms (Microsoft). Responses are recorded on the schools' MIS system against individual student accounts.

Where the Federation collects additional Biometric data, or begins to process the biometric data for a new purpose, new consent must be gained to ensure that the individual or their parent/carer is fully informed. This consent must also meet all of the standards outlined in this section.

The Protection of Freedoms Act 2012 only covers processing on behalf of the Federation. If a pupil is using biometric software for their own personal purposes (e.g. facial recognition technology) this is classed as private use not processing by the Federation, even if the software is accessed using school or college equipment.

5. Length of Consent and Withdrawing Consent

The consent will be valid until it is withdrawn or until the Biometric data reaches the Federation's retention period, as outlined in the Federation's retention schedule and individual school's Information Asset Register when the student leaves the School, at which point the Biometric data and record of consent will be securely destroyed.

Consent can be withdrawn at any time by the parent/carer or the individual, by emailing the individual school's Admin email address.

If a student under the age of 18 objects to the processing of their Biometric data, this will override the consent of the parents/carers and processing will not continue under any circumstances.

6. Alternative to Biometric Data

The Federation will ensure that where consent is refused or withdrawn there is an alternative solution which does not require the obtaining or processing of Biometric data. This will ensure that the consent is freely given and that no pressure is placed on the individual or their parent/carer to consent in order to take part in the Federation's processes.

7. Data Protection Impact Assessment

Where a new system involving Biometric data, or a new form of processing for Biometric data is introduced, the Federation will ensure that both schools have completed a Data Protection Impact Assessment (DPIA) to address any risks associated with the project prior to the implementation of the project. This will be sent to the School's Data Protection Officer for final approval.