

This Annex constitutes the School's Record of Processing Activities (ROPA) under Article 30 UK GDPR and includes details of processing purposes, lawful basis, data categories, recipients, retention periods, and security measures. ANNEX D TO DATA PROTECTION POLICY															
Legend As required: Only those who have a reason for access to data ('need to know') are granted access either by system permissions for soft records or by physical security for paper records. Admiss: Admissions Cont.: Contract under Article 6(1)(b) UK GDPR Con: Consent FOI: Freedom of Information Act Fin: Finance Hard: Paper records secured. Info: Information LI: Legitimate Interest LO: Legal Obligation under Article 6(1)(c) UK GDPR Mgr: Management Offr: Officer PI: Public Interest/Task under Article 6(1)(e) UK GDPR Sig: Signature(s) Soft: IT server with back up and physical security, password access as required, staff directives on data protection VI: Vital Interests The School is the Data Controller for all processing activities listed. Named roles are responsible for operational management of the data.															
Serial	Type of record	Why held	Categories of data subjects	Categories of personal data	Legal base	How or from where data collected	How data stored and protected	Security measures	How processed	Distributed to and why?	Internal Responsible Owner	Access by?	Retention period	Reason for length of period	DPIA
(a)	(b)	(c)			(d)	(e)	(f)		(g)	(h)	(i)	(j)	(k)	(l)	
1	Pupil Records (including on Bromcom and SIMS).	Pupil Management	Pupils, Parents / carers	Personal identifiers, Contact details, Educational records, Safeguarding data, SEN data, Health / medical data	LO	Application and new pupil forms	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Bromcom SIMS (archive) Data is limited to what is necessary for statutory and educational purposes. Irrelevant or excessive data is deleted or anonymised in accordance with retention policy.	Staff 'need to know'	Student Information Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	The later of: 6 years after the pupil has left the School or he/she reaches age 25.	1. To provide exam results where lost by pupil. 2. In order that any very late complaints may be investigated	No
2	Pupil Disciplinary Records that include permanent exclusion, permanent removal, exclusion when a Governors' panel is required to sit or any other case where there is a reasonable supposition that issues may be raised later. Governors' panel papers also to be retained. All other Pupil Disciplinary Records are to be treated as Pupil Records.	Pupil Management	Pupils, Parents / carers	Personal identifiers, Educational records, Disciplinary records	LO	During disciplinary cases	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, restricted physical access	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access	Bromcom SIMS (archive)	Staff, governors, parents as required	Student Information Officer; School Secretary	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	Date of birth + 25 years (or longer where safeguarding concerns apply)	For appeals and later queries. (NB a pupil raised issues about his exclusion 10 years after he left the School	No
3	GCSE/ 'A' Level results	Initially for pupil management & statistical reasons then as a service to pupils	Pupils, Parents / carers	Personal identifiers, Educational records	LO PI	Exam boards	Stored in locked cabinets with access restricted to authorised staff, copied to Bromcom, performance data	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Bromcom SIMS (archive)	Pupils & teaching Staff, support staff as required.	Exams Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	Permanent (summary record of attainment). Supporting documents retained in line with IRMS Toolkit (typically until pupil reaches age 25)	As a service for ex pupils who have lost their own.	No

3a	Assessment materials collected from students to support teacher assessed gradings at GCSE and 'A' level	Pupil Management	Pupils, Parents / carers	Educational records	LO	Classroom assessments	Stored in locked cabinets with access restricted to authorised staff	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Manually	Staff 'need to know' Examination board on appeal	Departmental head	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	3 months 12 months if appealed 24 months if appeal declined	For appeals and later queries.	No
4	Admiss Appeals – successful	Admiss Management	Pupils, Parents / carers	Personal identifiers, Educational records	LO	Appeal Panel	Stored in locked cabinets with access restricted to authorised staff	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Manually	Admissions Officer, HM, as required	Admission Appeals Officer	Admissions Officer, HM, Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	One year after admission	Any queries	No
5	Admiss Appeals – unsuccessful	Admiss Management	Pupils, Parents / carers	Personal identifiers, Educational records	LO	Appeal Panel	Stored in locked cabinets with access restricted to authorised staff	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Manually	Admissions Officer, HM, as required	Admission Appeals Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	Two years after appeal	Any further action	No
6	Register of Admission	Pupil Management	Pupils, Parents / carers	Personal identifiers, Educational records	LO	Initial pupil forms, common transfer form from primary school	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	As required	Admissions Officer, HM, as required	Student Information Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	Reduced record Permanent	For historic queries	No

7	Daily register	Pupil Management	Pupils, Parents / carers	Personal identifiers, Educational records	LO	By staff on daily registers	Stored securely on school systems with role-based access controls,	Role-based access controls, password-protected systems,	Attendance for each pupil generated in Bromcom	Stats to census, as required	Attendance Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system	As for Pupil Records above	As for Pupil Records above	No
8	Parental Data	Pupil Management	Pupils, Parents / carers	Personal identifiers, Contact details	LO	Application, new pupil forms, parental letters etc	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Basic data to Bromcom. Letters etc to pupil file	As required	Student Information Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	Retained as part of the pupil record where relevant; otherwise deleted 1 year after pupil leaves.	For any follow up action after the pupil has left.	No
9	Pupil Medical: permissions	Pupil Management & safeguarding	Pupils, Parents / carers	Personal identifiers, Health / medical data	LO, VI	New pupil forms & parental letters etc	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Data to Bromcom. Letters etc to pupil file As required	As required	Student Information Officer	Reception & Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	One month after event	For short term reference	No
10	Pupil Medical: Specific conditions	Pupil Management & safeguarding	Pupils, Parents / carers	Personal identifiers, Health / medical data	LO, VI	New pupil forms & parental letters etc	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Data to Bromcom. Letters etc to pupil file As required	DSL & staff as required	Student Information Officer	Reception & Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	One year after end of condition	For short term reference	No

11	Pupil Medical: Incidents	Pupil Management & safeguarding	Pupils, Parents / carers	Personal identifiers, Health / medical data	LO, VI	New pupil forms & parental letters etc	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Data to Bromcom. Letters etc to pupil file As required	DSL & staff as required	Student Information Officer	Reception & Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	As for Pupil Records above	To track whole pupil history	No
12	Pupil & parental data from pupil applications to join the School	Pupil Management	Pupils, Parents / carers	Personal identifiers, Contact details, Educational records	LO	Application forms	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	To Bromcom (Y7-11) or Appliaa (6F)	Admiss Offr for Lower & Mid school plus Network Mgr 6th form pastoral Offr SENCO for Spec Req	Admissions Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	20 school days after results of 11+ or other entry test 6th Form	Latest date for appeals 2 months after admission refused.	No
13	Child Protection and Safeguarding records.	Safeguarding	Pupils, Parents / carers, Third-party professionals	Personal identifiers, Safeguarding data, Health / medical data	LO	By all staff, especially pastoral staff, parents and any other agencies involved with a case	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted access via dedicated safeguarding system, strict role-based permissions, audit logging, encryption, secure backups, and multi-factor authentication for remote access.	Appropriate action by DSL	DSL & staff as required	DSL	By all staff, especially pastoral staff, parents and any other agencies involved with a case	Retained in accordance with statutory safeguarding guidance (Keeping Children Safe in Education), typically until the individual reaches age 25.		Yes
14	Biometric Data (thumb prints for cashless catering and registration). Neither is compulsory.	Staff/ Pupil Management	Pupils	Personal identifiers, Biometric data	Con, LO	Pupils	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Encrypted storage, restricted system access, secure deletion mechanisms, and strict access controls limited to authorised IT personnel.	Purchased S/W system	Nil	DPO	IT operation only	Deleted immediately pupil leaves the School or opts out of payment by this means	No longer required	Yes

15	Record of Dining Room purchases	Meal charging	Pupils, Parents / carers	Personal identifiers, Financial data	Cont., LI	Isometric identification	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure system access controls, restricted finance system permissions, encryption where applicable, and secure backups.	Purchased S/W system, Insight	Fin for accounting	Finance Manager	Pupil & parental access	6 Months	So parents can enquire	No
16	Trip and Visit Details	Pupil & Trip Management	Pupils, Parents / carers, Staff	Personal identifiers, Health / medical data, Contact details	LO, PI	Pupils and parents	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted access to authorised staff, secure storage systems, controlled sharing, encryption where appropriate, and secure disposal after use.	For permissions as required by Policy for trip	Staff notified of pupil absence Stats to Governors	EVC	EVC, Finance and Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	6 years	For accounting purposes	No
17	11+ Familiarisation And Study Skills Classes	Class management & success analysis	Pupils, Parents / carers	Personal identifiers, Contact details	Cont., PI	Parents	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	By Admin Sp	Tutors Fin	Admin Sp, Trips, Finance	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	2 years	To correlate class attendance with 11+ exam results	No
18	Other extra-curricular/ evening classes: Pupils	Class management	Pupils, Parents / carers	Personal identifiers, Contact details	Cont., PI	Applicants	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	By Admin Sp	Tutors Fin	Admin Sp, Trips, Finance	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	6 months after class unless advised will re-enrol.	For queries	No

19	Other extra-curricular/ evening classes: Tutors	Tutor Management	Staff	Personal identifiers, Employment data, Financial data	Cont., PI	Tutors	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.	Admin Sp	Admin Sp	Admin Sp, Trips, Finance	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	Later of date tutor advises will no longer take classes or 2 years from last class	For further employment	No
20	Sports Hall Lettings by individuals or representing organisations	Letting Management	Members of the public	Personal identifiers, Contact details, Financial data	Cont., PI	Letting application form	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure storage systems, controlled administrative access, financial system protections, encryption where appropriate, and secure backups.	Sports Hall Mgr makes bookings prog, to Fin for billing	Admin Sp, Fin	Admin Sp, Trips, Finance	Finance office	7 years after last letting	For accounting compliance	No
21	Other lettings for adult language classes, sewing club etc	Letting Management	Members of the public	Personal identifiers, Contact details, Financial data	Cont., PI	Letting application form	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure storage systems, controlled administrative access, financial system protections, encryption where appropriate, and secure backups.	Admin Sp records, allocates rooms, infos Fin	Admin Sp, Trips, Finance	COO/Bursar	Finance office	7 years after last letting	For accounting compliance	No
22	Basic employee record: start date, end date, reason for leaving, job roles.	Staff management	Staff	Personal identifiers, Employment data	LO	New staff form	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	To personnel file	As required	HR	Finance and HR office	20 years.	Provision of references, statistical historical purposes.	No

23	Personnel files including training records and notes of staffing, disciplinary and grievance hearings.	Staff management	Staff	Personal identifiers, Employment data, Disciplinary records, Performance data	LO	Collated from course etc	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	To personnel file	As required	HR	HR office	6 years from the end of employment	References and potential litigation.	No
24	Staff Health Questionnaire (at start of employment)	Staff management	Staff	Personal identifiers, Health / medical data	LO, VI	New staff form-	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	To personnel file	As required	HR	HR office	6 years after employment terminates	For reference	No
25	Staff Application forms/ interview notes.	Recruitment management	Staff	Personal identifiers, Recruitment data	Cont.	Applications	Stored in locked cabinets with access restricted to authorised staff	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	Interview panels	As required	HR	HR office and Access restricted to authorised staff based on role and 'need to know', enforced via system	6 months after interview (unsuccessful) 6 months after employment terminates (successful)	Time limits on litigation.	No
26	Facts relating to redundancies.	Staff management	Staff	Personal identifiers, Employment data	LO	Staff redundancy forms	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	By HR, Payroll, Pensions, Redundancy panel processes & Fin Payroll, Pensions, Fin, Panel members, TU officials or other 'friends'	As required	HR	Panel members and secretary	6 years from the date of redundancy.	Time limits on litigation.	No
27	Facts relating to redundancies where 20 or more redundancies.	Staff management	Staff	Personal identifiers, Employment data	LO	Staff redundancy forms	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	By HR, Payroll, Pensions, Redundancy panel processes & Fin Payroll, Pensions, Fin, Panel members, TU officials or other 'friends',	As required	HR	Panel members and secretary	12 years from the date of the redundancies.	Limitation Act 1980.	No

28	Statutory Maternity, Paternity Pay records and calculations.	Staff management	Staff	Personal identifiers, Payroll / tax data, Financial data	LO	Staff, GP	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	HR Input to payroll system, processed by Payroll	Nil	HR	Nil	6 years from the end of the tax year to which they relate.	Statutory Maternity Pay (General) Regulations 1986.	No
29	Staff Parental/ Adoption Leave.	Staff management	Staff	Personal identifiers, Payroll / tax data, Financial data	LO	Staff, GP (Adoption Agency/Social Services for adoption)	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	HR Input to payroll system, processed by Payroll	Nil	HR	Nil	6 years from birth/adoption of the child or 18 years if the child receives a disability allowance.	Time limits on litigation.	No
30	Statutory Sick Pay records and calculations.	Staff management	Staff	Personal identifiers, Payroll / tax data, Financial data	LO	Staff, GP etc	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	HR Input to payroll system, processed by Payroll	Nil	HR	Occupational Health if required	6 years from the end of employment.	Time limits on litigation	No
31	Wages and salary records (including overtime, bonuses and expenses).	Staff management	Staff	Personal identifiers, Payroll / tax data, Financial data	LO	HR, Staff	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	HR Input to payroll system, processed by Payroll	As required	HR	Finance and HR Office	6 years from end of employment	Taxes Management Act 1970.	No
32	Accident books, and records and reports of accidents.	Staff management	Staff	Personal identifiers, Health / medical data	LO	All staff	Stored in locked cabinets with access restricted to authorised staff	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	Analysed for trends	As required	COO/Bursar	Stats to governors, no access to personal data unless specific issue then as required	Books: later of 3 years after the date of the last entry or until age 21. Major Accident Reports: 10 years Minor Accident reports: 5 years Medical under COSH or asbestos: 40 years. Medical under ionising radiations Regs: later of 50 yrs or age 75	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985. Legal action	No

33	Staff Health Records where reason for termination of employment is connected with health.	Staff Management	Staff	Personal identifiers, Health / medical data	LO	Staff	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	Stats, for Governor's panels if nec	As required	HR	Governors medical panels if necessary	6 years from the end of employment.	Time limits on litigation.	No
34	Records relating to working time	Staff Management	Staff	Personal identifiers, Employment data	LO	Absence notified to HR	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	Stats for HM & Govs. To Fin for sick pay	As required	HR	Finance & HR Office	2 years from date they were made	The Working Time Regulations 1998 (SI 1998/1833)	No
35	Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999.	Staff Management	Staff	Personal identifiers, Health / medical data	LO	Heads of Depts storing/using such substances	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted HR system access, secure personnel files, encryption where appropriate, controlled access permissions, and secure backups.	Stored on staff personal files only accessed for relevant health issues	As required	HR, Student Information Officer	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	40 years.	Control of Substances Hazardous to Health Regulations 1999	No
36	Disclosure and Barring Service (DBS) records.	Staff Management	Staff	Personal identifiers, Criminal records data	LO	DBS	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Restricted access, secure storage, handling in accordance with DBS Code of Practice, and secure disposal after permitted retention period.	Accessed for new employees, governors, helpers etc	As required	HR	Access only if required - HR Office	6 months after recruitment decision		No

37	Governor Records	Governor management	Governors, Members / trustees	Personal identifiers, Governance records	LO	Governors	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Role-based access controls, password-protected systems, encryption where appropriate, secure backups, restricted physical access for paper records, and multi-factor authentication for remote access.		For Company's House, DfE	Clerk to the Governors	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	6 years but basic details: name, contact details, dates as governor, committees served on retained for historical purposes.	To allow for a request for references	No
38	Board Meeting Minutes	Governance	Governors, Members / trustees	Governance records	LO	At Committee meetings	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure storage systems, controlled access to authorised governance personnel, restricted access for confidential records, and secure backups.	Accessed as required.	Committee members and those in attendance	Clerk to the Governors	Anybody unless confidential under FOI	Ad infinitum	As required by Law	No
39	Board Meeting documentation	Governance	Governors, Members / trustees	Governance records	LO	As per Agenda requirements	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure storage systems, controlled access to authorised governance personnel, restricted access for confidential records, and secure backups.	Accessed as required.	Committee members and those 'in attendance	Clerk to the Governors	Anybody unless confidential under FOI	Ad infinitum if supporting strategic decisions taken. As for personnel files if support authority for pay rises, pay regrading or any other HR issue.		No
40	Company Records, Membership Certificates and Members' Meetings Minutes	Governance	Governors, Members / trustees	Governance records	LO	Company registration, on becoming a member, As per Agenda requirements	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure storage systems, controlled access to authorised governance personnel, restricted access for confidential records, and secure backups.	Accessed as required.	Committee members and those 'in attendance	Clerk to the Governors	Anybody unless confidential under FOI	Ad infinitum	As required by Law	No

41	Annual Reports	Governance	Governors, Members / trustees	Governance records	LO	Collated from current data	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Secure storage systems, controlled access to authorised governance personnel, restricted access for confidential records, and secure backups.	Accessed as required.	Companies House, DfE, Website	Clerk to the Governors	Anybody	Ad Infinitum	For historical research	No
42	CCTV Videos/ Images	Safeguarding & security	Pupils, Staff, Visitors	CCTV images / video	LO, PI	Cameras	Stored securely on school systems with role-based access controls, password protection, encryption where appropriate, regular backups, and multi-factor authentication for remote access.	Encrypted storage, restricted IT access, controlled viewing permissions, system monitoring, and automatic deletion after the defined retention period.	Not unless required to be	Staff, Police etc if required	Network Manager	Access restricted to authorised staff based on role and 'need to know', enforced via system permissions or physical controls.	30 days unless required for longer for a specific incident e.g. an offence being committed	To allow any incidents recorded to be viewed and retained if appropriate	Yes