



QUEENS' SCHOOL

Dare to be Great

Privacy Notice

Applicable to all members of the school community (past and present)
This Privacy Notice also forms the schools' Data Protection Policy

References

1.1 Legal and regulatory framework:

- UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- UK GDPR sits alongside the DPA 2018 and the Privacy and Electronic Communications Regulations (PECR) 2003 (as amended 2019)
- The Privacy and Electronic Communications Regulations (PECR) 2003 (as amended 2019), and ICO's Direct Marketing Guidance (2023) The Protection of Freedoms Act 2012

1.2 Relevant Guidance and practice notes provided by the Information Commissioner's Office:

This Privacy Notice also applies in addition to the School's other relevant terms and conditions and policies, including :

- The ICO Guide to the Privacy and Electronic Communications Regulations
- The ICO Guide to Direct Marketing
- The ICO Code of Practice on Subject Access
- The ICO Data sharing code
- The ICO Code of Practice on CCTV
- The ICO Code of Practice on Privacy Notices
- The ICO sector-specific guidance for schools, universities and colleges
- HM Government: Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (March 2015)
- Privacy Notices under the GDPR
- Direct Marketing Guidance (PECR) The ICO's Guide to Data Protection
- Overview of the General Data Protection Regulation
- DRAFT Consent Guidance for GDPR

1.3 Relevant School Policies:

This Privacy Notice also applies in addition to the School's other relevant terms and conditions and policies, including but not limited to :

- any contract between the school and its staff or the parents of pupils
- the school's policy on taking, storing and using images of children
- the school's CCTV policies
- the school's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded
- the ICT Acceptable Use policy and eSafety policies

2. General Principles

General Data Protection Regulation 2018 ("the Act") protects an individual's rights in respect of their information. Queens' School process large amounts of "personal data" about members of the school

community. Under the Act, the school must process such personal data "fairly and lawfully". This includes telling pupils and parents how their personal data will be held and used by the school. This Privacy Notice is intended to help meet that legal requirement. It should be noted, from the outset, that data protection should always take second place to safeguarding and child protection. If there is a potential conflict between the 2 competing requirements, the welfare of the child is paramount.

This notice does not apply to the practices of companies that we do not own or control, or to people that we do not employ or manage.

2.2 This Notice

This notice is intended to provide information about how the school will use (or "process") personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians (referred to in this notice as "parents"), staff and visitors. It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of personal data.

Anyone who works for, or acts on behalf of, the school (including staff, volunteers, trustees and service providers) should also be aware of and comply with this privacy notice, which also provides further information about how personal data about those individuals will be used. Further details are in Sections 3 and 4 of this notice.

2.3 Responsibility for Data Protection

In accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the school has notified the Information Commissioner's Office of its processing activities. The school's ICO registration is **Queens' School (Bushey) Ltd.** registration number **Z2837459** and its registered address is Queens' School, Aldenham Road, Bushey, Hertfordshire, WD23 2TY

Whilst Queens' School is the Data Controller for the school, the School has appointed a member of the Senior Leadership Team as a designated Data Protection Officer (DPO) as well as a Member of the Governing Body to act as a Data Protection Liaison Governor. The role of the DPO is to ensure that all personal data is processed in compliance with this notice and the Act.

The DPO acts independently and reports directly to the Governing Body.

Concerns should be raised first with the DPO, who will seek to resolve issues internally before escalation to the ICO.

In the event of queries, the DPO may be contacted at the School via :email : DPO@queens.herts.sch.uk
or telephone 01923 224465

or via written communication sent to the Data Protection Officer at the School postal address.

2.4 Principles of the UK GDPR

2.4.1 Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is :

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure

- personal data will not be transferred outside the UK unless appropriate safeguards are in place in accordance with Chapter V of the UK GDPR, such as adequacy regulations, International Data Transfer Agreements (IDTAs), or Addendums to the EU SCCs

2.4.2 Under GDPR, the following rights exist for individuals :

- Right to be informed how data is used by the School (as set out throughout this Privacy notice)
- Right of access to personal data held by the School
- Right of rectification where personal data can be rectified if it is inaccurate or incomplete
- Right of erasure also known as the “right of erasure” is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- Right to restrict processing in order to ‘block’ or suppress processing of personal data in certain circumstances e.g. where the data is inaccurate or the processing was unlawful, so that particular data is merely held but not processed
- Right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services
- Right to object to processing based on legitimate interests, direct marketing or processing for purposes of scientific/historical research and statistics
- Right to object to decisions made automated individual decision-making (making a decision solely by automated means without any human involvement)

2.5 Types of Personal Data Processed by the School

The school may process a wide range of personal data about individuals including current, past and prospective pupil, their parents and employees as part of its routine operation.

- names, addresses, telephone numbers, e-mail addresses and other contact details
- car details (about those who use School car parking facilities)
- bank details and other financial information, e.g. payroll details for members of staff
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks
- where appropriate, information about individuals' health, and contact details for their next of kin
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils as well as references supplied by previous employers of staff
- academic and professional qualifications as well as relevant previous experience and annual reviews of employees
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's policy on taking, storing and using images of children)

Generally, the school receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

2.6 Special category data

The school may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin,

political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

Examples in this category may include :

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so: for example for medical advice, social services, insurance purposes or to organisers of school trips
- To provide educational services in the context of any special educational needs of a pupil
- To provide spiritual education in the context of any religious beliefs
- In connection with employment of its staff, for example DBS checks, welfare or pension plans
- To run any of its systems that operate on photo ID data, such as for security and other forms of pupil identification (catering payment, library borrowing etc.); or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

2.7 Use of Personal Data by the School

The school will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its "legitimate interest" operations, including as follows :

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents
- For the purposes of staff selection and to confirm the identity of prospective members of staff (including statutory safeguarding checks)
- To provide education services (including support for Special Educational Needs), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance
- To give and receive information and references about past, current and prospective pupils, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT acceptable use policies
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

2.8 Data Accuracy and Security

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing. The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, ensuring that it is held in accordance with the Principles of the Act. All staff will be made aware of this notice and their duties under the Act.

2.9 Safeguarding Practice and Information Sharing

Whilst the General Data Protection Regulation places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

For further information, see HM Government's "Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers" (March 2015). The Local Safeguarding Children Board (LSCB) can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act 2004. This can only take place when the information requested is for the purpose of enabling or assisting the LSCB to perform its functions. Any request for information about individuals should be necessary and proportionate to the reason for the request and should be made to Designated Safeguarding Leads or Safeguarding Coordinator who must discuss any such request with the Data Protection Officer.

Occasionally, the school will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority), or to complete surveys issued by organisations to which it is affiliated to including the Department for Education. Much of the information supplied to these groups is anonymous in character. For the most part, personal data collected by the school will remain within the school, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records which are held and accessed only by the School Surgery, or otherwise in accordance with express parental consent; and
- pastoral or safeguarding files

However, a certain amount of any Special Educational Needs pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that this pupil requires.

Staff, pupils and parents are reminded that the school is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education and the Prevent Duty) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the school's Safeguarding Policy.

Once our pupils reach the age of 13, the law requires us to pass on certain information to Youth Connexions who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent/carers can request that only their child's name, address and

date of birth be passed to Youth Connexions. This right is transferred to the child once he/she reaches the age 16. This request should be put in writing to the DPO. For more information about services for young people, please go to our local authority website : <https://hertfordshire.gov.uk/services/youngpeople/>

We do not rent, sell or share personal information about you with other people or non-affiliated companies except where, in accordance with Data Protection Law, some of the school's processing activity is carried out on its behalf by third parties, such as IT systems, payment for purchases and school lunches, payroll providers, cloud storage providers etc. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

2.10 Right To Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO at DPO@queens.herts.sch.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

2.11 Rights of Access to Personal Data ("Subject Access Request")

Individuals have the right under the Act to access personal data about them held by the school, subject to certain exemptions and limitations set out in the Act. These rights are subject to exemptions under the Data Protection Act 2018, including where disclosure would adversely affect safeguarding or ongoing investigations. Any individual wishing to access their personal data should put their request in writing to the DPO. The school will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within statutory time-limits. If an individual believes that any information held on him or her is incorrect or incomplete, then they should write to the DPO as soon as possible. The School will promptly correct any information found to be incorrect.

Exemptions. All members of the school community should be aware that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts (though examiners' comments may, in certain circumstances, be disclosed), nor any reference given by the school for the purposes of the education, training or employment of any individual.

3. Data Protection for Staff

The aim of this section is to detail how the privacy notice might affect pupils and parents of Queens' School and should be read in conjunction with Section 2, General Principles.

3.2 Data Protection Protocols

The following Protocols must be adhered to at all times :

- Staff should only ever share information on a "need to know basis"
- Data protection should never be used as an excuse for not sharing information where necessary. The welfare of the child is paramount
- Seniority does not give an automatic right to information
- All emails may be disclosable
- Only keep data for as long as is necessary

3.3 Confidentiality

Any School information/records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless the School's prior written consent has been obtained. This requirement exists both during and after employment. In particular, such information for the benefit of any future employer.

The law states that where a teacher is facing an allegation of a criminal offence involving a pupil registered at the School, the teacher concerned is entitled to anonymity until the teacher is either charged with an offence or the anonymity is waived by the teacher. If publication is made on behalf of the School, the School, including senior management and trustees could be prosecuted. If a teacher is charged with such an offence, all communication must be directed through the Headteacher who will have authority to deal with the allegation and any enquiries to ensure that this restriction is not breached. If a member of staff is found to have breached (whether intentionally or otherwise) this duty, any accusations will be dealt with under the School's Disciplinary Procedure.

3.4 Off Site Access

See also the School's eSafety Policy which states that: "The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove sensitive personal data [as defined in Section 2 of this Privacy Notice] from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headteacher. Where a member of staff is permitted to download data off site it will need to be password protected.

There are exceptions where prior approval is not required :

- SIMS, the School's data management system, may be used on personal devices provided that the device is secure and password protected.
- For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader

3.5 Taking Photographs in Schools

The General Data Protection Regulation is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance. Photos taken for official school use may be covered by the Act and pupils and students should be advised why they are being taken.

3.5.1 Personal use – e.g. :

- A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album.
- Family members invited to the School Play or Concert where copyright restrictions do not apply and wish to video it.

These images are for personal use and the Data Protection Act does not apply.

3.5.2 Official school use:

Photographs of pupils or employees are taken for building passes or identification on school coaches. These images are likely to be stored electronically with other personal data and the terms of the Act will apply.

e.g. A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but will not breach the Act as long as the children and/or their guardians are aware this is happening and the context in which the photo will be used. Permission is sought through the Parental contract, at which time parents are given the option to opt out. Information on who might have opted out is held by the DPO. Staff may ask for details of who is on the list at any time.

3.5.3 Media use:

A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

[ICO's 2023 Taking Photos in Schools guidance](#)

3.6 What to do in the Event of a Suspected Data Breach

A personal data breach is “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service”. A personal data breach may mean that someone other than the school gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within the school or if a member of staff accidentally alters or deletes personal data.

Under the terms of the Act, the School has a statutory duty to report the breach to the Information Commissioner's Office within 72 hours. All personal data breaches, whether or not they are reported to the ICO, must be documented internally in the school's Data Breach Register, including details of the incident, decision, and corrective action. In some circumstances, those people whose personal data has been unlawfully shared need to be informed too.

In the event of a breach, the member of staff must notify the DPO as soon as possible and certainly within 24 hours of becoming aware of the breach. This notification must include at least :

- your name and contact details
- the date and time of the breach (or an estimate)
- the date and time you detected it
- basic information about the type of breach; and
- basic information about the personal data concerned

The DPO will then make a judgement on the best course of action which is likely to include notifying the Headteacher, plus the Designated Safeguarding Lead in the event that the data breach includes pupils' details, as appropriate.

4.1 Data Protection Impact Assessments (DPIAs)

The school conducts Data Protection Impact Assessments (DPIAs) for high-risk processing activities such as new IT systems, biometric data use, or surveillance technologies

4.2 Data Protection for Pupils and Family

The aim of this section is to detail how the privacy notice might affect pupils and parents of Queens' School and should be read in conjunction with Section 2, General Principles.

4.3 Keeping in Touch and Supporting the School

The school will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the school, including by sending communications by email and by post. Unless the relevant individual objects, the school may also :

- Share personal data about current and past parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the school community, such as the Queens' Parents Association
- Contact current and past parents and/or alumni by post and email in order to promote and raise funds for the school
- Collect information from publicly available sources about current and past parents' and former pupils' occupation and activities, in order to maximise the school's fundraising potential

Should you wish to limit or object to any such use, or would like further information about them, please contact the DPO in writing.

4.4 Subject Access Requests

In addition to the general principles outlined in Section 2 :

- Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. Pupils aged 13 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.
- A person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his behalf.

4.5 Pupils' Rights

The rights under the Act belong to the individual to whom the data relates. However, the school will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted. In general, the school will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school will maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example, where the school believes disclosure will be in the best interests of the pupil or other pupils.

Pupils are required to respect the personal data and privacy of others, and to comply with the school's IT Acceptable Use Policy and the School rules.

4.6 Queries and Complaints

If an individual believes that the school has not complied with this notice or acted otherwise than in accordance with the Act, they should utilise the school complaints procedure and should also notify the DPO. The school will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

An individual can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO) and more information on how to do this is available on their website :

<https://ico.org.uk/concerns/>

<https://ico.org.uk/global/contact-us/email/>

Or by writing to the Information Commissioner's Office (ICO) at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel (01626) 545 700.

However, the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.

5. Data Retention and Storage Guidelines

In these guidelines, "record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material will contain personal data of individuals as defined in the Act: but not all. Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

Retention schedules are aligned with the IRMS Information Management Toolkit for Schools (2024). Retention periods will be reviewed annually to ensure compliance with statutory and best-practice guidance.

5.2 Storage of Records

Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data - or any large quantity of data - should as a minimum be stored in folders where access has been restricted. Network passwords should be complex and subject to regular change. Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record. It is important to bear in mind, when creating documents and records of any sort (and particularly email), that at some point in the future those documents and records could be disclosed - whether as a result of litigation or investigation, or because of a subject access request under the Act.

Paper records should be stored in dry, cool, reasonably ventilated storage areas. Under the Act, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into

marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not. However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the Act.

5.3 Archiving and the Destruction or Erasure of Records.

Staff given specific responsibility for the management of records must ensure, as a minimum, the following :

- That records - whether electronic or hard copy - are stored securely as above, where possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;
- That important records, and large or sensitive personal databases, are not taken home or – in respect of digital data - carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary, in which case it should be subject to a risk assessment and in line with the eSafety policy (therefore written permission requested in advance less the exemptions listed);
- That questions of back up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual ad hoc action;
- That arrangements with external storage providers - whether physical or electronic (in any form, but most particularly "cloud-based" storage) - are supported by robust contractual arrangements providing for security and access;
- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and - in the case of personal data - necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and
- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely - with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them. For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Paper records should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks should be dismantled and destroyed. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely.

5.4 Retention of Personal Data

The school will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the school. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this notice is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the DPO at the School. However, please bear in mind that the school may have lawful and necessary reasons to hold on to some data.

Timescales for Retention The school will keep an archive copy of exam related student records for an indefinite period of time. This is to service requests from old students who need confirmation from the school of exam grades. Data Retention with Statutory Requirements Refer to this website for up to date timeframes: <https://www.gov.uk/guidance/data-protection-inschools/record-keeping-and-management>

5.4 Suggested Retention Periods

Pupil records

Document type	Retention period - minimum	Action at end of retention period	Further information
Secondary school pupil records: Pupil reports, Pupil attendance, Pupil behaviour and achievements, Pupil performance records, Pupil medical records:	Until the pupil's 25th birthday.	Dispose of records securely. If the pupil leaves to go to another school, transfer the records to that school. There is guidance on what to do if the school closes before the end of the retention period.	See The Education (Pupil Information) (England) Regulations 2005 for details of what to keep in the education record. Retain as detailed in section 2 of the Limitation Act 1980.
Special educational needs and disabilities (SEND), including any SEND statements and accessibility plans	Until the pupil's 30th birthday.	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years . Retain as detailed in section 2 of the Limitations Act 1980
Attendance and absence	Until the pupil's 30th birthday	Dispose of records securely, unless the document is subject to a legal hold. If the pupil leaves to go to another school, transfer the records to that school.	SEND code of practice: 0 to 25 years . Retain as detailed in section 2 of the Limitations Act 1980

Child Protection Concerns

Document type	Retention period - minimum	Action at end of retention period	Further information
Child protection files	Until the child's 25th birthday. If the file relates to child sexual abuse, retain until the child's 75th birthday.	Dispose of records securely. Child protection files should be passed on to any new school a child attends. This should be transferred separately from the main pupil file.	Should be stored in a separate child protection file. Keeping children safe in education sections 66, 67, 121 and 122. The Report of the Independent Inquiry into Child Sexual Abuse (IICSA), recommendation on access to records
Allegations of child protection against a member of staff, including unfounded allegations	Until the staff member's normal retirement age, or 10 years from the date of the allegation, whichever is later.	Dispose of records securely.	Keeping children safe in education Working together to safeguard children

Finance records

Document type	Retention period - minimum	Action at end of retention period	Further information
---------------	----------------------------	-----------------------------------	---------------------

Contracts	6 years from the last payment on the contract.	Dispose of records securely.	Section 2 of the Limitation Act 1980 .
Debtor's records	6 years from the end of the financial year.	Dispose of records securely.	Section 2 of the Limitation Act 1980 .
Debtor's records	6 years from the end of the financial year.	Dispose of records securely.	May include invoices, budgets, bank statements and annual accounts. Record keeping (VAT Notice 700/21) .

Governance records

Document type	Retention period - minimum	Action at end of retention period	Further information
Admissions	3 years from the admission date.	Dispose of records securely.	Working together to improve school attendance
Attendance registers	3 years from the date of entry.	Dispose of records securely.	Regulation 14 of the Education (Pupil Registration) (England Regulations 2006)
Annual governors report	10 years	Dispose of records securely.	The Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002 . Retain as detailed in section 2 of the Limitation Act 1980 .
Curricular record	At least one year	Dispose of records securely.	The Education (School Records) Regulations 1989 . Regulation 3 of the Education (Pupil Information) (England Regulations 2005)
Directors – disqualification	15 years from the date of disqualification.	Dispose of records securely.	The Education (Company Directors Disqualification Act 1986: Amendments to Disqualification Provisions) (England 2004)
Records of educational visits	10 years from the date of the visit. If there was an incident on the visit, retain the permission slips for all pupils and the incident report in the pupil record , or until	Dispose of records securely.	Health and safety on educational visits . Retain as detailed in section 2 of the Limitations Act 1980

	the pupil reaches the age of 25.		
School vehicles	6 years from the disposal of the vehicle.	Dispose of records securely.	Section 2 of the Limitation Act 1980 .
Statutory registers and compliance	Retention periods vary, for example: Memorandums of understanding should be retained for the life of the academy plus 6 years. Annual reports should be retained for 10 years from the date of the report. Board meeting records should be retained for 10 years from the date of the meeting.	Dispose of records securely.	May include annual reports and governance records. Companies Act 2006 contains information on which statutory registers to keep. Compliance guidance in the maintained schools governance guide . Compliance guidance in the academy trust governance guide . Academy trust handbook .

Health and safety records

Document type	Retention period - minimum	Action at end of retention period	Further information
Accessibility plans	Life of plan plus 6 years.	Dispose of records securely.	Retain as detailed in section 2 of the Limitation Act 1980 .
Accident records	3 years from the date of the accident.	Dispose of records securely.	Accidents involving pupils should be retained in the pupil record. Regulation 25 of the Social Security (Claims and Payments) Regulations 1979 .
Monitoring exposure to substances hazardous to health, including asbestos	5 years	Dispose of records securely.	Control of Substances Hazardous to Health Regulations 2002
Health surveillance records	40 years	Dispose of records securely.	Control of Substances Hazardous to Health Regulations 2002 Health surveillance - Record Keeping
Other health records of staff	While the worker is employed in your school.	Dispose of records securely.	Control of Substances Hazardous to Health Regulations 2002 Health surveillance - Record Keeping
Fire assessments	Life of the risk assessment plus 6 years.	Dispose of records securely.	Fire Service Order 2005 . Retain as detailed in section 2 of the Limitations Act 1980 .

Property records

Document type	Retention period - minimum	Action at end of retention period	Further information
Maintenance records	6 years from the end of the financial contract.	Dispose of records securely.	Record keeping (VAT Notice 700/21).
Title deeds	12 years from the end of the deed.	Dispose of records securely.	Section 2 of the Limitation Act 1980 .

Staff records

Document type	Retention period - minimum	Action at end of retention period	Further information
Copies of DBS certificates	Max of 6 months from the date of recruitment.	Dispose of records securely.	Keeping Children Safe in Education
Maternity pay records	3 years after the end of the tax year in which the maternity pay period ends.	Dispose of records securely.	The Statutory Maternity Pay (General) Regulations 1986 .
Pay records	3 years from the end of the tax year they relate to.	Dispose of records securely.	PAYE and payroll for employers: Keeping records .
Personnel files	6 years from termination of employment.	Dispose of records securely.	Section 2 of the Limitation Act 1980 .
Retirement benefits	A minimum of 6 years from the end of the year in which the accounts were signed	Dispose of records securely.	Regulation 15 of the retirement Benefits Schemes (Information Powers) Regulations 1995 .

SUGGESTED RETENTION PERIODS

Except where there is a specific statutory obligation to destroy records, it is misleading to treat these suggestions as prescriptive time limits. The figures provided are not intended to replace the need for thoughtful judgment or specific advice, depending on the circumstances.

The figures suggested in this table are, in most cases, guides as to what are periods of reasonable necessity that could be defensible if challenged. While case-by-case decision-making for documents would be ideal, practical considerations mean that regular pruning of records may not always be an acceptable use of school resources. It is therefore accepted that, at times, a more systemic or broad-brush approach is necessary.

EMAILS and DATA ON SERVER

- **Pupil account:** Disable upon leaving school. Delete after a year.
- **Staff account:** Routine deletion of historic emails and data after 2–3 years and disable account within 1 week of leaving school (staff can ask the DPO for a grace period to work through their accounts). Delete after a year.

SCHOOL-SPECIFIC RECORDS

- **Registration documents of the school:** Permanent (or until closure of the school).

- **Reports presented to the Governing Body:** Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently
- **Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies:** Date of the meeting + 3 years then review
- **Reports created by the Head Teacher or the Management Team:** Date of the report + a minimum of 3 years then review
- **Records created by SLT, heads of year and other members of staff with administrative responsibilities:** Current academic year + 6 years then review.
- **Correspondence created by SLT, heads of year and other members of staff with administrative responsibilities:** There may be data protection issues if the correspondence refers to individual pupils or members of staff. Date of correspondence + 3 years then review.

INDIVIDUAL PUPIL RECORDS

- **Admissions (application forms, assessments, records of decisions):** Retain for 2 years from the date of admission.

SAFEGUARDING

- **Policies and procedures:** Keep a permanent record of historic policies.
- **Accident/Incident reporting:** Retain for as long as any living victim may bring a claim. Civil claim limitation periods can be set aside in cases of abuse. Ideally, review files periodically if resources and qualified personnel allow.
- **Video recordings of meetings (e.g., one-on-one meetings, classes, counselling, or application interviews):** A shorter retention policy is acceptable, typically 3–6 months or immediately upon review by the DSL, depending on how quickly concerns are likely to arise.

CORPORATE RECORDS

- **Certificates of Incorporation:** Retain permanently or until the dissolution of the company.
- **Minutes, notes, and resolutions of boards or management meetings:** Retain for a minimum of 10 years.
- **Annual reports:** Retain for a minimum of 6 years.

ACCOUNTING RECORDS

- **Accounting records:** These are records that enable a company's accurate financial position to be ascertained and which give a true and fair view of the company's financial state.
 - **Minimum retention:** 6 years for UK charities and public companies, from the end of the financial year in which the transaction took place.
 - **Internationally:** Retention may be up to 20 years depending on local legal/accountancy requirements.
- **Budget and internal financial reports:** Minimum retention of 3 years.

EMPLOYEE / PERSONNEL RECORDS

- **Single Central Record of employees:** Keep a permanent record of all mandatory checks undertaken (do not keep the DBS certificate itself, which is retained for 6 months as above).
- **Contracts of employment:** Minimum retention of 7 years from the effective date of the end of the contract.
- **Job application and interview/rejection records (unsuccessful applicants):** Minimum retention of 3 months, but no more than 1 year.
- **Staff immigration records:** Minimum retention of 2 years from the end of employment.
- **Worker sponsor records:** Minimum retention of 1 year from the end of employment.

- **Low-level concerns records about adults (where applicable and under a school policy):** Regular review recommended to justify longer-term retention as part of safeguarding files.

Insurance Records

- **Insurance policies (private, public, professional indemnity):** Retain for the duration of the policy (or as required by the policy) plus a period for any run-off arrangement and coverage of insured risks. Ideally, retain until it is possible to calculate that no living person could make a claim.
- **Correspondence related to claims/renewals/notification regarding insurance:** Minimum retention of 7 years, depending on what the policy covers and whether historical claims could be made.

Environmental & Health Records

- **Maintenance logs:** Minimum retention of 10 years from the date of the last entry.
- **Accidents to children:** Retain for 25 years from birth, or longer for safeguarding incidents.
- **Staff use of hazardous substances:** Minimum retention of 7 years from the end of the date of use.
- **COVID-19 risk assessments, consent, etc.:** Retain legal paperwork (consents, notices, risk assessments) but not individual test results. This will be subject to further review.
- **Risk assessments (carried out in respect of the above):** Retain for 7 years from the completion of the relevant project, incident, event, or activity.

GDPR Records

- **Article 30 GDPR records of processing activity, data breach records, impact assessments:** Retain with no limit, as long as no personal data is held. However, these records must be kept up to date, accurate, and relevant

Privacy Support and Contact Information

If you have any questions or suggestions about our Privacy Notice, please contact our DPO :
email : DPO@queens.herts.sch.uk

Telephone 01923 224465

Write to Data Protection Officer
 Queens' School
 Aldenharn Road
 Bushey
 Herts. WD23 2TY

SLT: Mr Padgham

Committee: FPAR

Trustee approved: December 2025

Review date: December 2028

Queens' School (Bushey) Ltd (registered number: 076506090)