Queen's College, London &
Queen's College Preparatory School

Data Protection Policy

Due for review Summer Term 2025

Contents

1. Aims

This policy is aimed at all pupils (including those in EYFS), parents, alumnae and staff. It explains how Queen's College, London[1] uses personal information. The school and its staff are committed to treating personal data in a responsible, open and trustworthy manner.

The school aims to ensure that all personal data collected about staff, pupils, parents, governors, alumnae, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, in paper and electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.
It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials); • Identification number; • Location data; or • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

[1] Queen's College, London ("the school") consists of Queen's College ("the College"), located at 43-49 Harley Street; and Queen's College Preparatory School ("QCPS"), located at 59-61 Portland Place.

Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Data controller

The school processes personal data relating to parents, pupils, staff, governors, alumnae, visitors and others, and therefore is a data controller.

5. Roles and responsibilities

This policy applies to all staff employed by the school, and to any external organisation or individual working on its behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Council

The Council has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

5.2 Data protection co-ordinator: the Bursar

The school's primary point of contact for data protection is the Bursar, acting as Data Protection Co-Ordinator (DPC). The DPC liaises with the Information Commissioner's Office (ICO), monitoring and reporting on compliance.

The Bursar can be contacted on data protection matters as follows:

Email: bursar@qcl.org.uk

Post: Data Protection Co-Ordinator
Queen's College, London
43-49 Harley Street
London
W1G 8BT

If the Bursar is unavailable, the Head of Estates and Compliance acts as the deputy regarding data protection matters.

5.3 The Principal and Headmistress

The Principal (at the College) and Headmistress (at QCPS) act as the representative of the data protection co-ordinator on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy;
- Informing the school of any changes to their personal data, such as a change of address; and
- Contacting the DPC (the Bursar) in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - If they have any concerns that this policy is not being followed;
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
  - If there has been a data breach;
  - Whenever they engage in a new activity that may affect the privacy rights of individuals; and

- If they need help with any contracts or sharing personal data with third parties.,

6. Data protection principles

The GDPR is based on data protection principles with which the school must comply.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed; and
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- So that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract;
- So that the school can **comply with a legal obligation;**
- To ensure the **vital interests** of the individual or another person i.e. to protect someone's life;
- So that the school can **perform a task in the public interest;**
- For the **legitimate interests** of the school or a third party, provided the individual's rights and freedoms are not overridden; and/or
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent;
- To perform or exercise obligations or rights in relation to employment, social security or social protection law;

- To ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made manifestly public by the individual;
- For the establishment, exercise or defence of legal claims;
- For reasons of substantial public interest as defined in legislation;
- For health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- For public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law; or
- For archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent;
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made manifestly public by the individual;
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights; and
- The data needs to be processed for reasons of substantial public interest as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals concerned when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This is to be carried out in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
  - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share; and
  - Only share data that the supplier or contractor needs to carry out their service.

We will share personal data with law enforcement and government bodies where we are legally required to do so.

We may share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

In the unlikely event that we need to transfer personal data internationally, we will do so in accordance with data protection law.

9. Data subject access requests and other rights of individuals

9.1 Data subject access requests (DSAR)

The law provides for a right enjoyed by all individuals – including parents, pupils and staff (past, present and prospective) – to know what personal data about them is being held and used ("processed" in GDPR jargon) by organisations, including schools. This is subject to certain limitations and exemptions, but these rules can be time-consuming to apply. In general, the school should expect to go to considerable lengths, time and expense in dealing with DSARs, especially in tricky and complicated cases.

The DSAR is not the same as a parent's statutory right to receive a copy of their child's educational record under the Education Act 1996; this is sometimes cited by parents, but **it does not apply to independent schools**.

Individuals have a right to make a DSAR to gain access to personal information that the school holds about them. The definition of personal data is wide, and includes emails, correspondence, minutes, reports, results, databases (e.g. SchoolBase, including secure notes), lists and expressions of opinion. Specifically, the right includes:

- Confirmation that their personal data is being processed;
- Access to a copy of the data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been, or will be, shared with;
- How long the data will be stored for or, if this isn't possible, the criteria used to determine the retention period;
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- The right to lodge a complaint with the ICO; and
- The source of the data, if not the individual themselves.

Two further rights are unlikely to apply to the school, but are included for completeness:

- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual; and
- The safeguards provided if the data is being transferred internationally.

DSARs can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- The name of the individual making the DSAR;
- Their correspondence address;
- Their contact number and email address; and
- Details of the information requested.

If staff receive a DSAR in any form they must immediately forward it to the Bursar and ensure that the Principal or Headmistress (as appropriate) are informed. The Bursar will inform the Chair of Council as quickly as possible. In the absence of the Bursar for more than 24 hours (e.g. on holiday), the Assistant Bursar will lead the response to the DSAR until the Bursar returns to work.

The response time specified by the law is one calendar month, starting from the date that the request is actually received (**not** sent). In some cases this can be extended by a further two

months "where necessary" (a factor of the complexity of compiling the required response and the number of requests), provided the reasons for the extension are communicated to the data subject within the first month. In practice, this rule is largely un-tested and it would not be wise to assume that it will apply; in particular, inconvenience (for instance if the DSAR is received during the school holidays) is not a relevant factor in whether an extension would be merited.

9.2 DSAR on behalf of a pupil

A DSAR may be made on another person's behalf – for example, by their authorised solicitor, or a parent. It should not, however, be assumed that parents have that authority.

Personal data about a child belongs to that child, and not the parent. A child of any age has the same right to make a DSAR as an adult. However, in practice a person with parental responsibility (a parent or carer) will normally exercise those rights on behalf of a child "too young to understand the nature of the requests" (in most cases, until the age of 12 for a child of average maturity, though each case should be judged on its merits).

If the parent of a child aged 12 or above makes a DSAR with respect to their child, the school must receive written and signed consent from the child for the personal data to be disclosed to the parent.

9.3 The formal requirements for a valid DSAR

The law does not set many rules about this: a DSAR does not have to mention the GDPR, the DPA, or use any of the technical jargon of data protection law. It does not even have to be in writing (though see 9.2 above about consent if the request is made on someone else's behalf). It simply needs to be clear that the requester wishes to access information about themselves which the school holds.

Similarly, the motive for the request is irrelevant; even if the person simply wants to dig around and see what they might find (for instance in the context of a current or likely complaint or legal claim), that is still a valid exercise of the right.

A DSAR can validly be made to anyone in the school, by any written means (including digital, which is why the school has strict rules for staff to have Out of Office auto-replies switched on when they are away).

9.4 Responding to a DSAR

A detailed process for responding to a DSAR can be found at Appendix 3.

9.5 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests;
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to the ICO; and
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Bursar, in his capacity as Data Protection Co-Ordinator. If staff receive such a request, they must immediately forward it to the Bursar.

10. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Bursar or the Premises Manager.

11. Photographs and video

As part of our school activities, we may take photographs and record images of individuals within the school.

When a pupil first joins the school we obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. For pupils aged 18 or over, we obtain this consent from the pupils themselves. We clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where the school takes photographs and videos, uses may include:

- Within the school on notice boards and in Queen's Today, brochures, newsletters, etc.;
- Outside the school, for instance in publicity material or development campaigns; and

- Online on our school website or social media pages.

When using photographs and videos we do not accompany them with any other personal information about the pupil, to ensure they cannot be identified.

Consent can be refused or withdrawn at any time; if consent is being withdrawn after initially being granted, this should be done in writing to the Principal or Headmistress (as appropriate) or the Bursar. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

Unless consent is withdrawn in this way, the initial consent is deemed to apply throughout the pupil's time at QCPS or the College; we do not seek consent every year.

Photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, before each event attended by parents we specifically request that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons.

12. Data protection by design and default

We have measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPC (the Bursar), and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Bursar will advise on this process);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
- Regularly conducting reviews and audits to test our privacy measures and check we are compliant; and publishing privacy notices for the benefit of data subjects, which set out all information we are required to share about how we use and process their personal data, and include the name and contact details of the school and the Bursar (as DPC).

13. Data security and storage of records

We protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:
Paper-based records and portable electronic devices, such as laptops and hard drives that

contain personal data, are kept under lock and key when not in use;

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access;
- Where personal information needs to be taken off site, staff must sign it in and out from the school office;
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites;
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use of Technology policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context might include, but are not limited to:

- Safeguarding information being made available to an unauthorised person; or
- The theft of a school laptop containing non-encrypted personal data about pupils.

16. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPC is responsible for monitoring and reviewing this policy. This policy will be reviewed every year and shared with the full Council.

18. Links with other policies

This policy should be read in conjunction with:

- Acceptable Use of Technology policy;
- Safeguarding policy;
- Staff Code of Conduct;
- Staff Privacy Notice;
- Alumnae Privacy Notice;
- Pupil Privacy Notice; and
- Parent Privacy Notice.

Appendix 1: Data Retention Schedule

The table below sets out the periods for which specified information and data records must be retained. The list is not exhaustive and where a particular retention guide does not exist, staff are expected to apply best practice by retaining data for no longer than is necessary. Further guidance can be sought from your Head of Department or a senior member of staff, the Bursar, or the Head of Estates and Compliance.

Once a retention period has expired the data **MUST** be erased.

Type of Record / Document	**Retention Period**
Governance Records	
Registration documents	Permanent (or until closure of the school)
Attendance register	6 years from last date of entry, then archive
Minutes of Council	6 years from date of meeting
Curriculum	3 years from the end of the academic year
Other class records (e.g. marks, timetables)	1 year from end of the academic year
Pupil records	
Admissions: application forms, assessments, records of decisions	25 years from date of birth if pupil admitted 7 years from decision if pupil not admitted
Examination results (external or internal)	7 years from pupil leaving school
Pupil file including: - Reports - Performance records - Medical records	25 years from date of birth. **Any material which might be relevant to potential safeguarding cases or potential claims should be retained for the lifetime of the pupil.**
SEN records (to be risk assessed individually by SENCO)	Date of birth plus up to 35 years (to allow for special extensions to statutory limitation period).
Safeguarding	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates	**No longer than 6 months** from date of decision on recruitment, unless DBS specifically consulted. N.B. A record of the checks being made must be retained, if not the certificate itself.
Accident / Incident reporting	Keep on record for as long as any living victim might bring a claim. Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available[2].

[2] N.B. civil claim limitations may be set aside by the Courts in cases of abuse. The High Court has found that a retention period of 35 years was within the bracket of 'legitimate approaches'. It also found that it would be

Type of Record / Document	Retention Period
Child protection files	If a referral has been made or social care has been involved or the child has been the subject of a multi-agency plan: **indefinitely** If low-level concerns and no multi-agency involvement: apply the school's low-level concerns policy: 25 years from date of birth
Accounting[3]	
Accounting records[4]	UK Charities: a minimum of 6 years from the end of the financial year in which the transaction took place
Tax returns	Minimum of 6 years
Budget and internal financial reports	Minimum of 3 years
Contracts and Agreements	
Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments)*	Minimum of 7 years from completion of the contractual obligations or the term of the agreement, whichever is the later.
Deeds (*or contracts under seal*)	Minimum of 13 years from completion of the contractual obligation or the term of the agreement.
Intellectual property records	
Assignments of intellectual property to or from the school	Expiry of right + 7 years for contracts Expiry of right + 13 years for deeds
IP/IT agreements (including software licenses & ancillary agreements – e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum of 7 years from completion of obligation under term of contract / non-contract agreement
Personnel records	
Single Central Record of employees	Retain a permanent record of all mandatory checks that have been undertaken (not the certificate)
Contracts of employment	7 years from effective date of end of contract
Staff appraisals or reviews	Duration of employment + minimum of 7 years
Staff personnel file	Duration of employment + minimum of 7 years **– BUT do not delete any information which might be relevant to historic safeguarding claims**
Payroll, salary, maternity pay records	Minimum 6 years

disproportionate for most organisations to conduct regular reviews, but the ICO still expects to see a 'reasonable assessment policy' (e.g. every 6 years) in place.

[3] Retention is for tax purposes, and is driven by legal / accountancy guidelines rather than data protection law.

[4] Defined as "*records which enable the school's accurate financial position to be ascertained and which give a true and fair view of the school's financial state*".

Type of Record / Document	Retention Period
Pension & other benefit schedule records	Possibly permanent, depending on nature of scheme
Job application and interview/rejection records	Minimum 3 months: **maximum 1 year**
Immigration records	Minimum 4 years
Health records relating to employees	7 years from end of contract of employment
Insurance Records	
Insurance Policies	Duration of policy (or as required by the policy) **plus** a period for any run-off arrangement and coverage of insured risks: ideally, **until it is possible that no living person could make a claim**
Correspondence related to claims / renewals / notification re: insurance	Minimum 7 years
Facilities and Health & Safety Records	
Maintenance logs	10 years from date of last entry
Accidents to children[5]	25 years from date of birth (unless safeguarding incident)
Records of accidents at work (staff)[5]	Minimum 4 years from date of accident, **but** review case-by-case where possible
Staff use of hazardous substances[5]	Minimum 7 years from end of date of use
Risk assessments carried out in respect of above[5]	7 years from completion of relevant project, incident, event, or activity

[5] Latent injuries can take years to manifest themselves, and the limitation period for claims reflects this: a note should be retained of all procedures as they were at the time, with a record that they were followed. Relevant insurance documents should also be retained.

Appendix 2: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Bursar (in his capacity as DPC).
- The Bursar will investigate the report, and determine whether a breach has occurred. To decide, the Bursar will consider whether personal data has been accidentally or unlawfully:
  - Lost;
  - Stolen;
  - Destroyed;
  - Altered;
  - Disclosed or made available where it should not have been; or
  - Made available to unauthorised people.
- The Bursar will alert the Principal (College) or Headmistress (QCPS) (as appropriate) and the chair of Council.
- The Bursar will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).
- The Bursar will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Bursar will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Bursar will consider whether the breach is likely negatively to affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data;
  - Discrimination;
  - Identify theft or fraud;
  - Financial loss;
  - Damage to reputation;
  - Loss of confidentiality; or
  - Any other significant economic or social disadvantage to the individual(s) concerned.

  If it's likely that there will be a risk to people's rights and freedoms, the Bursar must notify the ICO.
- The DPO will document the decision (just in case it is challenged at a later date by the ICO or an individual affected by the breach) and stored it in OneDrive[6].

[6] OneDrive – Queen's College London / 6. Administration / Data Protection & GDPR / Incident Logs & Docs

- Where the ICO must be notified, the Bursar will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the Bursar will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned; and
    - The categories and approximate number of personal data records concerned.
  - The name and contact details of the DPC;
  - A description of the likely consequences of the personal data breach; and
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the Bursar will report as much as he can within 72 hours. The report will explain that there is a delay, the reasons why, and when the he expects to have further information. The Bursar will then submit the remaining information as soon as possible.
- The Bursar will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high the Bursar will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - A description, in clear and plain language, of the nature of the personal data breach;
  - The name and contact details of the DPC;
  - A description of the likely consequences of the personal data breach; and
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

  Any decision on whether to contact individuals will be documented by the Bursar.
- The Bursar will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Bursar will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts relating to the breach;
  - Effects; and
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

  Records of all breaches will be stored in OneDrive (see above concerning documented decisions).
- The Bursar and Principal or Headmistress (as appropriate) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Appendix 3: Data Subject Access Request checklist

Section 9 describes Data Subject Access Requests (DSAR) in general terms, including what constitutes a valid request, the rules about consent and submitting a DSAR on someone else's behalf, and the data access rights of every individual. This Appendix is designed to provide more understanding and to act as a checklist for what to do when the school receives a DSAR.

What needs to be searched?

All digital systems under the school's control (OneDrive/Office 365, SchoolBase, Firefly, Sage), and any hard copy 'filing system' within the GDPR definition (e.g. hard copy safeguarding files, pupil files etc.). 'Digital systems' will include personal computers, mobile devices, text / WhatsApp accounts, and personal email of staff or Governors **if there is reason to think that they have been used for school business** and that such a search will recover the requester's personal data.

In theory, unstructured folders, files or notepads should fall outside this definition; however, if a file name or description carries enough identifying criteria to link it to a certain person (or a complaint or case involving them), and its content is structured enough for their personal data to be readily retrieved, then it should be searched.

If in doubt, include it and then refine the selection at the redaction stage.

Can we be proportionate in our approach?

Searches should be made for names but also known identifiers such as nicknames, initials, and alternate spellings. Keep in mind that searches for first name alone, surname alone and first name and surname together will often produce different (if overlapping) results; we need to do them all.. Searches must also include draft documents, local files, and supposedly "deleted" material that is still readily accessible via central IT systems.

The school is not allowed to narrow the scope of the request unilaterally, but we can make reasonable assumptions – based on the context and wording of the request – about the requester's primary areas of concern in terms of the personal data they hold, rather than always searching as widely as possible by default. We may also use some proportionality in applying exemptions: for example, if we consider that there is good reason to think a whole file will be privileged, we need not search within it.

We must apply proportionality with great care. If a requester does not receive everything they want, they can come back and ask for it, with or without involving the ICO. However, not every requester will be unreasonable, or want to pore over piles of irrelevant print-outs. Some may prefer to receive more targeted information sooner, which is why step 5 below attempts to clarify the scope by engaging directly with the requester. If they refuse, then at least the school can show the ICO which party has tried to be reasonable.

What information must we disclose?

A law only provides the right to access someone's own "personal data". Experience since the introduction of the DSAR suggests that the ICO defines this widely to include opinions, records of intentions, and anything that relates to a living individual who can be identified

in context. **Using abbreviations, nicknames, codes, etc. in our everyday business would not give the school any basis for avoiding disclosure.**

All the same, the right only relates to personal data, not whole documents or reports. A search for someone's name may throw up numerous results – but just because someone is mentioned in one email, or an attachment, or even the subject line, it does not render the entire email chain their personal data. Nor do we need to provide repeated copies of the same personal data: searches may return multiple versions of a document, but a single copy may be adequate to disclose (but be careful of multiple iterations of a draft; if the personal data materially changes from version to version, then each must be disclosed).

It is a criminal offence to change the meaning and nature of the data. However, the data does not have to be disclosed in its original format: it could be cut and pasted into a table, written out, or faithfully described.

How should we disclose the data?

It does not matter how the data is delivered, **provided it is intelligible to the requester** – it could be compiled in a table or single document, or scanned or photocopied from originals and sent digitally or in hard copy. Where scans or copies of originals are used, check carefully that redactions are unreadable under light and/or on a computer screen (particularly if the redaction was done with a pen before copying).

It is vital that the response is delivered securely, and to the right person. The preferred method for an electronic response is to set up a folder in OneDrive and use sharing permissions to ensure that the folder is accessible ONLY to the person managing the response and to the requester. Set a time-limit on the folder and inform the recipient that you have done so in the covering letter: "this folder will remain open until [Time] and [Date]".

If responding in hard copy, the best way to ensure safe delivery is by agreeing a time and method with the requester. Post, even by special or recorded delivery, is less secure than a courier (because it involves the risk of bundles of sensitive papers being returned to sorting offices if not signed for) – which in turn is less secure than collecting or delivering in person.

A vital part of the response is the covering letter. Stage 30 below sets out what should be included, However, we can also use the letter to manage the requester's expectations about what they are getting, and what they are not getting, while ensuring its contents are consistent with this policy, the school's privacy notices and the approach taken with exemptions.

What about CCTV images?

The school's CCTV cameras capture personal data in the form of images which must be provided if requested – but **a CCTV search is necessary only if specifically requested**. If the requester asks for CCTV images, the school is entitled to require them to be reasonably specific about location and time.

Providing CCTV footage to the requester needs very careful thought, especially around identifying third parties (see below): offering to show the person footage on-site is safer than sending out copies.

What if the information also identifies other people?

Where personal data about the person making a DSAR also constitutes "personal data" about another person (a "third party"), the school is not obliged to disclose this mixed data in response to a DSAR unless either (a) the third party has consented or (b) it is "reasonable" to disclose without their consent, taking into account all the relevant circumstances. Relevant factors will include the third party's known views, any harm or distress that may come to them by being identified, any reasonable expectations of (personal) confidentiality, and what the requester knows already.

Another factor is who the third parties are. **It will almost always be appropriate to protect the identity of other parents and pupils: even if known to the requester, this personal data should be minimised before it leaves the school's control**. It may also be fair to protect the identities of outside professionals, but **staff should assume that they will be named**.

What about the school's own confidential data?

There is no specific protection for information the school considers confidential in a commercial or corporate sense. Confidentiality can be a factor, but only in certain specific circumstances – namely:

- References provided confidentially, whether academic or professional;
- Management planning or forecasting (e.g. planned redundancies);
- Confidential negotiations with the requester (i.e. the school's intentions in offering settlement);
- Where legal privilege applies (see step 16); and
- Where a third party's data is confidential in a personal sense – e.g. medical, or clearly private and sensitive.

Should we include assessment or exam results, marks and scripts?

The law prevents the use of a DSAR to obtain exam results (which includes marked-up scripts, provisional marks, marking notes) ahead of time: where such data is disclosable, the response need not be provided until 40 days have elapsed from the formal announcement of such results or, as an absolute backstop, 5 months after the request is made.

Exam scripts – the information actually recorded by candidates during an exam – are not covered by DSAR requests, although markers should be wary that comments they make about a person on their scripts (i.e. where it is the personal data of the candidate, and not simply a comment or mark) could still be disclosable.

"Exam" can be interpreted widely to include all tests to determine a candidate's knowledge, intelligence, skill or ability, including in music, art or drama – so recordings of a performance could be counted as "exam scripts".

Can we require requesters to treat what we provide under the DSAR as confidential?

To a limited degree: it is good practice, and helpful, to indicate in the cover letter what the school deems to be confidential, and – if the file does contain third party data – stress this fact, and remind the recipient that they now have legal responsibilities for how it is used. However, to the extent that the information provided is the recipient's personal data, the law says that it is their information to use. This is another reason to confine disclosure to personal information only.

Actions to be taken on receiving a DSAR

Phase 1: Receipt

1. Inform the Bursar that you have received a DSAR and forward it to him/her as soon as possible. If the Bursar is not available (e.g. on holiday), inform the Principal or Headmistress as appropriate.
    a. The Principal or Headmistress should inform the Chair of the Council in all cases;
    b. If the Bursar is available, he will lead the response process; if he is not available, the Principal or Headmistress will appoint a manager to oversee the response process;
    c. Consider whether to hire temporary administrative support.
    Assuming you are the response manager:
    d. Respond to the requester, formally acknowledging receipt; at this stage do not confirm the deadline for responding. [See 3.a., 3.c, 6 and 7];
    e. Consider who else needs to know (e.g. Deputy Head (Pastoral), SENCO, appropriate Head of Section / Year, Nurse etc.);
    f. Alert the Head of IT and the Data Manager that a DSAR has been received so that they can start to design their searches;
    g. Contact the school's legal advisors, telling them that a DSAR has been received and that they should expect to be consulted in due course; and
    h. Establish a confidential folder in OneDrive, setting permissions so that it is accessible only to the Bursar, Principal or Headmistress (as appropriate), Assistant Bursar and the person managing the response; include sub-folders entitled "In Scope" and "Out of Scope".

2. Is Queen's a controller of the requester's data? (i.e. does Queen's, whether jointly or with others, determine the purposes and means of the processing of personal data?)
    a. If yes (which is the likely answer), move to Step 3;
    b. If no, then processors (those who process personal data on behalf of the controller) are not required to comply. Write to the requester to explain why we think we are a processor and not a controller. This response should confirm the right to complain to the ICO. *Always obtain legal advice on this matter; it is* ***extremely*** *unlikely that we will receive a DSAR from someone for whom we are not a data controller.*

3. Is the request from the requester or a third party?

    a. If from the requester, are you satisfied as to their identity? If not, ask for I.D. If this paragraph applies, then the deadline for the response starts from the date that the I.D. was confirmed. [See also 3.c.]
    b. If from a third party (e.g. a lawyer), have we received sufficient evidence of their authority to submit the request? If not, request a copy.
    c. If a parent (or someone acting *in loco* parentis) has submitted a request to be given access to the daughter's personal data:
        i. Is the daughter 12 years or older?
        ii. If no, then the parent is entitled to request on their behalf;
        iii. If yes, then write to the daughter direct (copying the requester), explaining that you have received a DSAR from their parent and seeking **written and signed** confirmation that the daughter consents for us to release the data to the parent. In this case, the deadline for responding starts from the date that the school receives written consent from the daughter. [See also 3.a.].
        iv. **Note:** if either 3.a. or 3.c. applies to this case, then write to the requester again once I.D. and/or consent has been received, setting out the response deadline.

4. Are there grounds not to comply with the request (i.e. the request is unfounded or is manifestly excessive)? *N.B. In practice this is unlikely; in any event, do not make such a decision without first obtaining specialist legal advice.*

    a. If so the school may charge a reasonable fee for account administrative costs.
    b. If we refuse to comply with the request, then we must give our reasons to the requester **and** tell the data subject that if there is a dispute then they may complain to the ICO and/or apply to the courts.

5. Has the DSAR set out the scope of the request? If not, then we should clarify the scope of the search in order to help locate the data.

    a. Are hard copy documents requested?
    b. If electronic searches are required:
        i. Has a date range to be searched been provided?
        ii. Have electronic search terms been provided?
        iii. Have specific locations (e.g. particular mailboxes) been requested?

        If **any** of i–iii are missing go back to the data subject / requester for clarification.
    c. If possible, agree the format of the eventual response (i.e. are you going to send the final results in electronic form or hard copy?). A hard copy response should be discouraged if possible, since it is much more time consuming, harder to control, collate and redact, and is likely to waste a huge quantity of paper. See step 28.
    d. If possible, maintain polite, professional contact with the requester; on no account treat them as an enemy or a threat. The law entitles them to make this request; we

must respond accordingly, however inconvenient and time-consuming it may feel.

6. Are there any grounds for seeking a further two-month extension in which to respond?
    a. Are there multiple requests from the same individual? (This means data requests; parallel processes which are **not** under GDPR / DP – such as the school's complaints procedure – do not count)
    b. Is the request complex (e.g. data locating would involve considering a large number of different mailboxes and dealing with and redacting a lot of third party data)? If so, write to the requester within the initial one month period to confirm use of the extension. *N.B. In practice, this is a high bar; inconvenience alone is not sufficient grounds for extending.* ***Obtain specialist legal advice before making a decision****.*

7. Write to the requester / data subject to confirm the deadline for responding (one calendar month from the date the DSAR was received, unless 3.a, 3.c and/or 6 apply).

8. Put the deadline for responding into your diary and that of:
    a. The Chair of Council;
    b. The Principal or Headmistress (as applicable);
    c. The Bursar (if he is not leading the response process).

9. Ensure that everyone involved in searching has clear instructions about what to do with the outputs (format, location, file naming conventions, etc.). In particular the outputs of email searches will arrive as a .pst file (readable only via Outlook). Converting each email to pdf with a suitable file name is extremely time-consuming and a good use of external temporary administrative support. N.B. once converted retain access to the original emails because it is much easier to redact in Word than after conversion to pdf.

Phase 2: Conducting the searches

10. Is there a request for on-line searches?
    a. If so, instruct the IT Manager and Data Manager to search using the terms defined in the request (or the subsequent clarification under 5.b.) to collate initial results;
    b. Ensure to include both live data and deleted and/or archived data if still held on a Queen's system or server.

11. If the request includes a search of hard copy documents locate documents for review.

Phase 3: Initial sift of documents

12. Does the document contain any personal data on the data subject (i.e. data from which the data subject can be identified with or without further information held by the school [as data controller]; examples include name, email, contact details, initials, nickname);
    a. If yes, move to step 13;
    b. If no, the document has no personal data on the data subject and does not need to be disclosed in the response.

13. Is the document already present elsewhere in the search results? (A common example is in disclosing email chains, where we should disclose the final message in the chain, having checked that all previous messages in the conversation are included. It is not necessary to separate the conversation into a separate document for each email.)
    a. If it is a duplicate, then there is no need to disclose it again;
    b. If it is not a duplicate, move to step 14.

14. Reading the document, is the data subject the subject or focus of the email? What is the email about? Is it discussing the data subject (either alone or included with other subject), or is it about another topic?
    a. If the data subject is the subject or focus, move to step 15;
    b. If the data subject is not the subject or focus of any part of the email, it is not disclosable.

Phase 4: Exemptions from disclosure

15. Is the document for purely personal or household activity? *[N.B. This is extremely unlikely in the context of Queen's]*
    a. If yes, the document is not disclosable;
    b. If no, move to step 16.

16. Is the document legally privileged (i.e. between Queen's College and a lawyer for the purpose of seeking legal advice)? This also covers all documents in which the school could maintain privilege in legal proceedings, including employment tribunals – provided the documents were prepared by the school or others for the purpose of the proceedings, or for a prospective claim (hence privilege may also apply to discussions with insurers). This does not apply to quasi-legal processes, such as the school's internal complaint, grievance or appeals processes ***[N.B. Always seek legal advice on this matter]***
    a. If yes, the document is not disclosable;
    b. If no, move to step 17.

17. Does the document attract litigation privilege (i.e. is it communication between Queen's College and a lawyer made for the dominant purpose of litigation, whether pending, reasonably contemplated or existing**? *[N.B. Always seek legal advice on this matter.]***
    a. If yes, the document is not disclosable;
    b. If no, move to step 18.

18. Does the document contain personal data processed for the purposes of management forecasting or management planning, where disclosure would prejudice the conduct of the school? This must be "ongoing management activity" to qualify. ***[N.B. Always seek Legal advice on this matter.]***

a. If yes, the document is not disclosable;
b. If no, move to step 19.

19. Is the document exempt, being in relation to ongoing negotiations with the data subject where disclosure would prejudice the discussions? *[N.B. these are genuinely legal discussions or negotiations; for example, the school's complaints procedure does not meet this criterion].*

    a. If yes, the document is not disclosable;
    b. If no, move to step 20.

20. Is the personal data for a reference given for employment or training purposes?

    a. If yes, the document is not disclosable;
    b. If no, move to step 21.

21. All documents that remain are disclosable: collate all documents not excluded during steps 12 – 20 in preparation for the redaction phase.

Phase 5: Redactions

This phase should be completed only after sifting documents via steps 12-21 above.
N.B. It is not realistic to expect temporary administrative support to perform redaction because they lack the requisite authority and knowledge of the school. The process is likely to require significant input from senior staff, particularly the Principal or Headmistress, Bursar and Pastoral teams.

22. Does the email or attachment contain any third party data?

    a. If yes, move to step 23;
    b. If no, move to step 26.

23. Has the third party consented to disclosure?

    a. If yes, no redactions are needed; move to step 26;
    b. If no, move to step 24.

24. Would disclosure as part of the response be likely to cause any harm (mental or physical) to any third party?

    a. If yes, we need to balance such risk of harm with the data subject's right of access. If the balance tilts towards likely harm to the third party move to step 25.
    b. If no, no redactions are needed; move to step 26.

25. Can harm to the third party be removed by redacting the third party's details?

    a. If yes, redact and move to step 26;
    b. If no, the document is not disclosable.

26. Does the document contain and commercially sensitive information which the school (as data controller) would not want to disclose? *[N.B. In practice, this is unlikely to apply in the context of Queen's. Always seek legal advice if you are considering using this clause].*
    a. If yes, is it in relation to current sensitive information not in the public domain? If so, consider redacting;
    b. If already in the public domain, no need to redact.

27. Now collate all the outputs of the search following redaction (do not forget those which did not require any redaction).

Phase 6: Sending the final response and covering letter.

28. Does the personal data need to be provided in electronic form? *[Where possible agree this at the outset – see 5.c.]*
    a. If requested to be provided in hard copy, print all outputs and prepare for despatch. *[N.B. there will probably be a considerable volume of material]*;
    b. If the request does not specify, then the law states that the data should be provided "in a commonly used electronic format". Use pdf.

29. Always get legal support and advice in drafting the covering letter.

30. Attach a covering letter specifying:
    a. The purposes of the processing;
    b. The categories of personal data concerned;
    c. The recipients or categories of recipient to whom the personal data have been or will be disclosed – particularly recipients in third countries or international organisations. ***[N.B. be careful of this post-Brexit, depending on the outcome];***
    d. Where possible, the period for which it is envisaged that the personal data will be stored [see Appendix 1 of the Data Protection Policy]; if not possible, state the criteria used to determine that period;
    e. The existence of the right to request that Queen's College (as data controller) rectify or erase personal data or restrict processing of personal data concerning the data subject, or to object to such processing;
    f. The existence of the right to lodge a complaint with the ICO;
    g. Where the personal data were not collected from the data subject, any available information as to their source *[this is unlikely to apply in the context of Queen's]*;
    h. *[This clause is very unlikely to apply to Queen's; simply state that no automated decision-making or profiling has taken place]* The existence of automated decision-making, including profiling, and (at least in those case) meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
    i. *[This clause unlikely to apply to Queen's; simply state that no personal data has been*

*transferred to a third country or to an international organisation – though **be careful post-Brexit**]*
Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Appendix 4: Data Protection Impact Assessment (DPIA) query form

The live copy of this form is located in Firefly

Staff Name:

Staff Job Title:

Date:

Description of activity
Purpose of the activity
What personal data will be involved?
How long will the personal data be kept?
What are the potential personal data risks?
How will the personal data be protected?
Where will the data be stored (if on-line, in which country)?