Queen Elizabeth's School
DATA PROTECTION POLICY

1. AIMS

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

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

The School needs to collect and process pupil and staff data in order to:

- Support teaching and learning
- Monitor and report on pupils' progress
- Provide appropriate pastoral care
- Protect children from harm
- Assess and monitor special educational needs
- Provide prompt and appropriate management in the case of illness
- Assess the School's overall performance
- Ensure the effective administration of the School
- Fulfil contracts of employment with staff
- Comply with all statutory and other legal requirements

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the School's use of biometric data and 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, individual. This may include the individual's: • Name (including initials) • Identification number • Location data

	• 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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, for example including information about an individual's: • Racial or ethnic origin • Religious or philosophical beliefs • Trade union membership • Biometrics • Health – physical or mental
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. THE DATA CONTROLLER

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

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by the School, and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action in line with the School's Staff Disciplinary Procedures.

5.1 Governing Body

The Governing Body has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities to the Governing Body and, where appropriate, report their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the School processes, and for the ICO.

The School's interim DPO is Mr. M Rose and is contactable at the School via dpo@qebarnet.co.uk or on 02084414646.

5.3 Headmaster

The Headmaster acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

i) Collecting, storing and processing any personal data in accordance with this policy;

ii) Informing the School of any changes to their personal data, such as a change of address; and

iii) Contacting the DPO 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 they know or suspect a data breach;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals; or

- 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 that the School must comply with. The principles say that personal data must be:

i) Processed lawfully, fairly and in a transparent manner;

ii) Collected for specified, explicit and legitimate purposes;

iii) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;

iv) Accurate and, where necessary, kept up to date;

v) Kept for no longer than is necessary for the purposes for which it is processed; and

vi) 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

The School will only process personal data where it has one of six 'lawful bases' (legal reasons) to do so under data protection law:

i) The data needs to be processed 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;

ii) The data needs to be processed so that the School can comply with a legal obligation – including an obligation arising under the Freedom of Information Act 2000;

iii) The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life or wellbeing;

iv) The data needs to be processed so that the School, as a public authority, can perform a task in the public interest, and carry out its official functions;

v) The data needs to be processed for the legitimate interests of the School or a third party; or

vi) The individual (or their parent when appropriate in the case of a younger pupil) has freely given clear consent.

For special categories of personal data, the School will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Where the School offers online services to pupils, such as eQE, and intends to rely on consent as a basis for processing, it will secure parental consent where the pupil is under the age of 12.

Whenever the School first collects new personal data directly from individuals, it will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

The School will only collect personal data for specified, explicit and legitimate reasons. These reasons will be explained to the individuals when that data is first being collected.

If the School wants to use personal data for reasons other than those given when first obtained, it will inform the individuals concerned before doing so, seek additional and specific consent where necessary.

Staff must only process personal data where it is necessary in order to fulfil their duties.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done with reference to guidance from the Information and Records Management Society.

8. SHARING PERSONAL DATA

The School will not normally share personal data with anyone else, but may do so where:

i) There is an issue with a pupil or parent that puts the safety of other pupils or staff at risk;
ii) The School needs to liaise with other agencies to fulfil its statutory obligations or for core educational functions, such as the DfE, UCAS or HMRC.
iii) Clear consent has been provided by the data subject (or their parent in the case of a younger pupil), where consent forms the legal basis for processing that data;
iv) Suppliers or contractors need data to enable the School to provide services to pupils and staff – for example, IT companies who deliver the School's information management systems. When doing this, the School will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data shared; and
- Only share data that the supplier or contractor needs to carry out their service.

The School will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy our safeguarding obligations; or

- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The School may also share personal data with the emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or members of staff.

Should there be a planned transfer of personal data to a country or territory outside the European Economic Area, this will be done so in accordance with data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds about them. This includes:

i) Confirmation that their personal data is being processed;

ii) Access to a copy of the data;

iii) The purposes of the data processing;

iv) The categories of personal data concerned;

v) Who the data has been, or will be, shared with;

vi) How long the data will be stored for, or if this isn't possible, the criteria used to determine this period;

vii) The source of the data, if not the individual; and/or

viii) Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- The name of the individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO. The DPO will take appropriate steps to verify the identity of the individual making the access request before releasing the relevant personal data.

9.2 Pupils and subject access requests

Personal data about a pupil belongs to that pupil, and not the pupil's parents. For a parent to make a subject access request with respect to their son, the pupil must either be unable to understand their rights and the implications of a subject access request, for example due to age, or have given their express consent.

Pupils aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at the School may not be granted without the

express permission of the pupil. However, a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Parents, as defined under Education Law, have a right to be involved in decisions related to their son's education, including receiving an annual report of progress in the main subjects taught. As a registered academy, the School is not legally obliged to provide parental access to a pupil's School Record, but may agree to do so in certain circumstances upon request, such as if a pupil is being excluded. The School will comply both with data protection law and its policy on Dealing with issues relating to Parental Responsibility.

9.3 Responding to subject access requests

When responding to requests, the School:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and within 1 month of receipt of the request;
- Will provide the information free of charge;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual;
- Would reveal that the pupil is at risk of abuse, where the disclosure of that information would not be in the pupil's best interests;
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, the School may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. Where a request is refused, the School will explain to the individual why this decision has been taken and inform them of their right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information about how data will be used and processed upon collection, individuals also have the right to:

i) Withdraw their consent to processing at any time;

ii) Ask the School to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);

iii) Prevent use of their personal data for direct marketing;

iv) Challenge processing which has been justified on the basis of public interest;

v) Request a copy of agreements under which their personal data is transferred outside of the European Economic Area;

vi) Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);

vii) Prevent processing that is likely to cause damage or distress;

viii) Be notified of a data breach in certain circumstances;

ix) Make a complaint to the ICO; and/or

x) 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. BIOMETRIC RECOGNITION SYSTEMS & BIOMETRIC DATA SECURITY

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, the cashless payment systems in the dining hall and School Shop) we will comply with the requirements of the Protection of Freedoms Act 2012. Under this legislation, an individual is considered to be a child if they are under the age of 18.

Parents will be notified before any biometric recognition system is put in place or before their son first takes part in it. The school will obtain clear consent from at least one parent before any biometric data is collected and processed.

Parents and pupils have the right to choose not to use the school's biometric system. The School will consider alternative means of accessing the relevant services for pupils in those circumstances.

Parents and pupils can object to participation in the School's biometric recognition system, or withdraw consent, at any time, at which point the School will ensure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the School will not process that data, irrespective of any consent given by the pupil's parents.

Where members of staff use the School's biometric systems, their consent will also be obtained before they first take part in it. Staff can also withdraw consent at any time, and the School will delete any relevant data already captured.

Whilst the School utilises unique biometric identifiers with respect to the Dining Hall, School Shop and 'follow-me' printing functions, the School does not hold or itself process biometric data. The School has written assurances that BioStore, provider of the unique identifier database management system, meets the requirements of the GDPR and Data Protection Act 2018 in the processing, storage, transfer and deletion of data relating to these processes.

11. CCTV

The School uses CCTV in various locations around the school site to ensure it remains safe. In doing so, the School will be informed by the ICO's code of practice for the use of CCTV.

The School does not need to ask individuals' permission to use CCTV, but will make it clear where this is in operation. Cameras will be clearly visible and appropriate signage will be employed. Only the Headmaster and Assistant Heads will have access to CCTV footage and recordings overwrite on a rolling monthly basis with footage only retained where there is good reason to do so, such as an incident whereby disciplinary action has been necessary.

Data will be securely stored and will not be shared with third parties unless there is a strong justification for this, such as to provide evidence in a criminal investigation. CCTV will not be utilised in places that would reasonably be expected to be private, such as bathrooms and changing areas. Further details can be found in Appendix 2.

12. PHOTOGRAPHS AND VIDEOS

As part of School activities, photographs and recorded images may be taken.

The School will obtain written consent from parents, via the Home School Agreement and in additional specific cases where required, and from pupils aged over 18 for photographs and videos to be taken of pupils for communications, marketing and promotional materials.
The School will clearly explain how the photographs and/or videos will be used.

For example, uses may include:

- Within School on notice boards and in school magazines, brochures, newsletters, etc.;
- Outside of School by external agencies such as the School photographer, newspapers to whom the School has supplied images, and other campaigns;
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, steps will be taken to delete the photograph or video and not distribute it further.

13. DATA PROTECTION BY DESIGN AND DEFAULT

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

i) Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;

ii) 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);

iii) Completing privacy 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 DPO will advise on this process);

iv) Integrating data protection into internal documents including this policy, any related policies and privacy notices;

v) Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters;

vi) Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant; and

vii) Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of the School and the DPO and all information required about how we use and process personal data (via privacy notices)
- For all personal data held, maintaining an internal record of the type of data, data subject, how it is processed, why it is processed and the period of retention.

14. DATA SECURITY AND STORAGE OF RECORDS

The School will take all reasonable steps to 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 securely when not in use;
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- Visitors are required to sign-in, wear identification when on site and will be escorted by a member of staff, if appropriate;
- Where personal information needs to be taken off site, staff must maintain equally rigorous forms of data protection;
- Strong passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals;
- Security software is in place and kept up to date, with secure data back-ups, and agreements are in place with any third party providers around data security;
- Staff are only able to access personal data relevant to their role at the School;
- Access to computer rooms is controlled by keypad entry;
- Encryption software is used to protect portable devices and removable media, such as laptops and USB devices, where needed to protect personal data;

- Staff, pupils or governors who store personal information on their own devices are expected to follow the same security procedures as for school-owned equipment;
- Staff and pupils must act in accordance with the School's ICT Policy and its requirements in terms of data protection, portable and cloud-based data storage and acceptable use;
- The School and the DPO should be notified immediately should a pupil or member of staff have evidence or suspicion that there is a data vulnerability or a breach has occurred; and
- Where the School needs to share personal data with a third party, due diligence is carried out and reasonable steps taken to ensure it is stored securely and adequately protected (see section 8).

15. 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 the School cannot or does not need to rectify or update it.

For example, the School will shred or incinerate paper-based records and overwrite or delete electronic files. The School may also use a third party to safely dispose of records on its behalf. If doing so, the School will require the third party to provide sufficient guarantees that it complies with data protection law.

Records will be disposed of once the data is no longer needed for its originally intended use, its legal basis has expired, and it is beyond any retention period required by law.

16. PERSONAL DATA BREACHES

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

Identifying a data breach

All staff should be familiar with the following examples of data breaches and how to identify them and training should be given to staff on this at regular intervals.

A personal data breach can be broadly defined as a security incident that affects the confidentiality, integrity or availability of personal data – or put another way, wherever personal data is lost, destroyed, corrupted, disclosed or accessed in error or if the data is unavailable and this has a significant negative impact on the individuals whose data it is.

In practical terms, data breaches may include but are not limited to:

- unauthorised access/hacking of the School's IT systems (whether located at our premises or in the cloud);
- lost or stolen computers or portable devices containing any data relating to our School;

- lost or stolen papers such as trip information with passport details, home addresses and nationality;
- inadvertent disclosure of any School information to any recipient for whom it was not intended. This could include:
    - an attachment on an email being sent to the wrong email address;
    - disclosure of information being given out to a parent or supplier in error;
    - disclosure of information to a third party where the correct permissions were not in place;
- disclosure to an unauthorised person as a result of 'phishing' where someone has impersonated a known parent/supplier by email or on the telephone;
- unauthorised use of School information by a member of staff without the correct permissions (whether deliberate or not); or
- a security incident similar to the above affecting our supplier data processors which we are notified about. (Under the GDPR, our suppliers are required to notify data breaches to us without undue delay);
- A non-anonymised dataset being published.

All of the above should be considered potential data breaches and reported to the DPO in accordance with the protocol set out in Appendix 1. Some of these breaches will carry more risks than others – for example, the loss of information that contains key identity information about someone (e.g. a copy of a passport) or if the information is particularly sensitive (e.g. if it relates to Safeguarding or SEND (Special Educational Needs and Disabilities) information.)

This list is not exhaustive and if there is any doubt on what constitutes a data breach, the DPO should be consulted immediately. When appropriate information has been gathered, the School – most likely via the DPO - will report the data breach to the ICO, but in all circumstances within the 72 hour legal deadline. Multiple communications may be made to the ICO, following an initial report, as further details become known.

Spam email folders must be checked daily to ensure no data breaches notified to us by suppliers are missed. At least two members of the School's IT team should have signed up to receive relevant email notifications on all updates and patches that are required to keep School systems up to date (including those of our data processor suppliers) and our IT team should also consider what data feeds might be appropriate to ensure they are kept up to date with relevant press reporting in this regard.

In the unlikely event of a suspected data breach, the School will follow the procedure set out in Appendix 1.

17. FREEDOM OF INFORMATION

Data requests can still be made in writing to the School under the Freedom of Information Act 2000 and the School will comply with its duties as set out in this legislation. FOIs will be centrally co-ordinated and a record of requests and responses will be maintained. If information is already in the public domain, the School may inform the requester accordingly – with the School routinely publishing key information via its website. Other information requests will be handled with reference to the procedures set out in Appendix 3, noting that personal data may need to be exempted or redacted from a Freedom of Information response in order to avoid breaching individuals' rights under data protection law.

18. TRAINING

All staff 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, with all staff being required to complete essential training related to the GDPR.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing the School's policy and procedures with regards to data protection, in consultation with other relevant members of staff. However, any substantial changes proposed to the policy will require the approval of the Governing Body, in line with the School's wider approach to setting and reviewing policies.

The policy will be reviewed at least every 2 years, in line with guidance from the Department for Education.

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

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

Step 1: Identifying a data breach and containing the risk

- On finding or causing a breach, or potential breach, **the staff member or data processor must immediately (within the hour) notify the DPO and the Headmaster.** There must be no delay in reporting the data breaches – even a delay of 24 hours is not acceptable.

Examples of common data breaches are set out in section 16 of the Data Protection Policy above. The information in question may or may not contain personal data and may or may not merit reporting externally but that is not an assessment that should be made by anyone but the DPO, with legal advice as necessary.

- **The data breach must not be discussed with any third parties without express permission from the DPO.** Discussing data breaches in contravention of this requirement can lead to increased risks for the affected individuals and increase the School's liabilities and may be a disciplinary offence.

- **The DPO will confirm receipt of the complaint to the reporting staff member.** If the staff member has not received an acknowledgement within this timeframe, they must escalate this by reporting it to the Headmaster. **The DPO must make arrangements during all planned absences** for a deputy with the appropriate permissions.

- **The DPO will investigate the report immediately** (same day), and determine whether a breach has occurred as well as assessing the potential consequences and how likely they are to happen. It is critical that the DPO finds out as much information about the purported breach as possible. All information divulged must be recorded in writing as soon as possible (e.g. by making contemporaneous notes of phone calls). All such notes should be password protected and stored in a secure file location. **The DPO must also identify the external and internal policies and contracts which may be relevant to the breach.** For example, in the case of a stolen laptop, the staff policy on using portable devices must be consulted. **In tandem with this, the DPO must consult with colleagues** to see if any disciplinary action or additional training should be considered.

- **To investigate the breach, the DPO will complete and follow the initial Risk Assessment** set out at the end of this Appendix. A log of this Risk Assessment should be password protected and stored in the secure file.

Step 2: Internal reporting

- **The DPO will alert the Headmaster and the Chairman of Governors of the result of the initial Risk Assessment (the same day) with a recommendation for internal reporting. If the DPO needs assistance with the Risk Assessment, they should contact relevant senior members of staff.** The data breach must not be discussed with any third parties. If there are any comments on the Risk Assessment,

these should be recorded – it is important that the School has all the relevant facts in one place as the Risk Assessment will help form the basis of parent, pupil and regulator communications and to assist the School in handling the consequences of the breach.

Step 3: External reporting

- **The DPO will work out whether the breach must be reported to the ICO or to other external parties including affected parties. This must be judged on a case-by-case basis using the Risk Assessment criteria and the Headmaster should be informed before the report is submitted**. To decide, the DPO will consider whether the breach is likely to negatively 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;
    - Unauthorised reversal of pseudonymisation;
    - Damage to reputation;
    - Loss of confidentiality; or
    - Any other significant economic or social disadvantage to the individual(s) concerned.

- This can be a complex assessment and the School may need legal advice. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPO will document the decision, either way, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are to be password protected and stored in a securely kept central electronic register.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours of becoming aware of the breach. A copy of this report should be password protected and saved in the secure file. As required, the DPO 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 DPO;
    - 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 DPO will report as much as they can within 72 hours.** The ICO recognises that with data breaches, it often takes some time to aggregate all the facts – for example where a system intrusion has been detected but it is not clear what data may have been accessed or taken. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

- **The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact to establish if we need to notify them. Of particular importance is whether the affected individuals could be at risk of identity theft, card fraud or if the data involved is sensitive or encrypted**. This is a higher threshold than the test for notifying the Information Commissioner but there may also be good reasons to notify at least the affected individuals – if an email has been sent in error to several parents for example, then generally the error should be explained to the parents on that email as they will already be aware of the breach.

- **If we decide not to notify individuals this should be recorded in the breach case notes.** It may be advisable to take legal advice on this and the ICO may also be able to give guidance. The risk assessment should assist. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO;
    - 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.

- The **DPO will notify any relevant third parties** who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies. If there has been evidence of a theft or fraud then the School should alert the police. See: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime. These other pages may also be helpful: https://www.met.police.uk/ro/report/ocr/af/how-to-report-a-crime/. **If it is decided that the School does not need to report a crime, we still need to be able to justify this decision and should document it in the breach case notes**.

- The DPO must consider (in consultation with the Headmaster) whether the media should be alerted and how this is done – this is very unlikely to be required however. If inaccurate press reports are circulated this must be addressed with the Headmaster's Office and it may be sensible to consider obtaining external professional advice.

Step 4: Evaluation and Lessons Learned

- **The DPO will document each breach, irrespective of whether it is reported externally**. For each breach, this record will include the:
    - Facts and cause;
    - 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).

- The DPO and Headmaster will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. The DPO must agree a memorandum for the Headmaster (and Governing Body if serious) to approve which sets out the lessons learned from the data breach and a timetable for addressing any compliance issues that require improvement.

Recommendations may include: a review of policies, internal documents and forms, websites, suppliers, IT systems and budgets, staff reporting structure, staff roles, staff training; the establishment of steering groups and committees; more 'dummy runs' testing, business continuity and greater penetration testing. Costings for recommendations should be given wherever possible so the necessary budgets can receive sign off. Consideration may be given to the below:

Question	Answer	Remedial action
Were procedures and preparations sufficient?		
Were policies and lines of responsibility clear?		
Did detection occur promptly?		
Could additional tools or resources have helped?		
Was the incident sufficiently contained?		
Was communication adequate?		
Were staff sufficiently aware of data protection issues?		
What practical difficulties were encountered?		

Queen Elizabeth's School
DATA PROTECTION POLICY

DATA BREACH RISK ASSESSMENT (TO BE USED IN CONJUNCTION WITH DATA BREACH PLAN)

Breach Details: Please provide full details of all known details about the breach, citing the source and relevant date(s) the data was provided. A chronology of events is useful to establish the timescale so please provide all relevant dates. You may need to append separate continuation sheets if necessary.	
Type of and Number of Data Records Affected: e.g. name, email address, financial data, medical records, sensitive data such as criminal convictions, medical details, special educational needs or safeguarding details, religious beliefs or details of sexuality. Give a % of the relevant database affected where relevant.	
Location of relevant contracts and policies: e.g. provide file location (or attach a copy) of relevant parent contract, staff contract, supplier contract, internal policies. Summarise relevant contractual obligations if possible.	
Summary of Status: e.g. provide a summary of all conversations and emails that have occurred, the status of any internal or external report/investigation, when we can expect further information (what and when).	
Payment Data: Is payment information compromised? If so, please provide details of where the affected data is stored and by whom and whether any card providers have been notified.	
Likely Consequences: Please list the likely consequences of the data breach on each of the following: (i) affected individuals (e.g. could they suffer identity theft, card theft or personal embarrassment from disclosure of the data); (ii) the School (e.g. have we lost an important IT system and how long will it take to resume normal service)?	
Data Processors: Please list all data processors involved in the data breach (stating whether they caused the breach or will be otherwise impacted/need to be notified) – e.g. system suppliers. Please provide contact details for the relevant account representative who may be contacted.	

Queen Elizabeth's School
DATA PROTECTION POLICY

Involvement of Authorities: Please list whether we have received any request for information from any public authorities such as the ICO or the police relating to the data breach and the status of those requests.	
Steps taken to contain the breach:	
Steps taken to remedy the breach:	
Insurers notified?	
HR action required?	
Relevant locations: Specify where the data breach occurred (e.g. the location of the server on which the breached database is stored/the location where the device was stolen as applicable depending on the breach)	
Website links to media reports (if applicable):	
Risk Rating and Recommendations:	Need to notify ICO? Y/N (specify reasons)
	Need to notify police? Y/N
	Need to notify affected individuals and suggested method of communicating breach:
	Potential business risks (and classification of risk from 1 (low) – 5 (high):
Other information: Please provide any other information that you feel is helpful.	

Queen Elizabeth's School
DATA PROTECTION POLICY

Name of Person completing the form:

……..

Date: ……..

APPENDIX 2: CCTV POLICY STATEMENT

Introduction

1. The School uses closed circuit television (CCTV) images to reduce crime and monitor the School buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to School property. The images may also be used to determine the times at which staff and/or pupils enter and leave the School's premises.

2. The system is comprised of a number of fixed and dome cameras.

3. The system does not have sound recording capability.

4. The CCTV system is owned and operated by the School and the deployment of the system is determined by the School's leadership team.

5. The CCTV is monitored by the Facilities Manager using web-based software. The Headmaster and Deputy Heads also have access and the ability to monitor the CCTV footage.

6. Any changes to CCTV monitoring will be subject to consultation with staff and the School community.

7. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

Statement of intent

8. The School complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

9. CCTV warning signs are clearly and prominently placed at all external entrances to the School, including the gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV.

10. The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Siting the cameras

11. Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with data protection law.

12. The School will make every effort to position cameras so that their coverage is restricted to the School premises, which may include outdoor areas.

13. CCTV will not be used in changing rooms and toilets.

14. Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert monitoring

15. The School may in exceptional circumstances set up covert monitoring. For example:

    - Where there is good cause to suspect that an illegal or unauthorised action(s) is taking place, or where there are grounds to suspect serious misconduct;
    - Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

    In these circumstances authorisation must be obtained from the Headmaster. Covert monitoring must cease following completion of an investigation.

16. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

Storage and retention of CCTV images

17. Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

18. All retained data will be stored securely.

Access to CCTV images

19. Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available. The staff authorised to view the images are the Headmaster, Deputy Heads and the Facilities Manager.

Subject Access Requests (SAR)

20. Individuals have the right to request access to CCTV footage relating to them.

21. The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

Access to and disclosure of images to third parties

22. There will be no disclosure of recorded CCTV data to third parties other than to authorised personnel such as the police and service providers to the School where these would reasonably need access to the data (e.g. investigators).

23. The data may be used within the School's discipline and grievance procedures as the School considers appropriate, and the data will be subject to the usual confidentiality requirements of those procedures.

Complaints

24. Complaints and enquiries about the operation of CCTV within the School will be dealt with under the School's Complaints Procedure (GOVINF27).

APPENDIX 3: FREEDOM OF INFORMATION PROCEDURES

1. A valid FOI request should be in writing, state the enquirer's name and correspondence address and describe the information requested.
2. Requests for information not directly relating to a data subject should be referred in the first instance to the School Office where they will be logged before passing to an appropriate member of staff (usually the Headmaster).
3. In order to channel the request appropriately, the following will be considered:
    - Under which legal framework has the request been made
    - Whether the School holds the information requested.
4. At all times the School has a legal duty to provide advice and assistance to anyone requesting information.
5. If information is already in the public domain, this should be made clear to the enquirer.
6. If the information is held at the School, the staff member should
    - Consider whether a third party's interests might be affected by disclosure and if so, consult them.
    - Consider whether any exemptions apply and whether they are absolute or qualified.
    - Carry out a public interest test to decide if applying the qualified exemption outweighs the public interest in disclosing the information.
    - Decide whether the estimated cost of complying with the request merits a charge (and whether a charge may legally be made).
7. If a request is made for a document that contains exempt personal information, this information must be removed before supplying the document.
8. If the request appears to be vexatious or persistent the School may not be obliged to comply with the request.
9. FOI requests should be dealt with within 20 days (excluding school holidays) or 40 days if a qualified exemption applies and the School is required to consider the public interest test.
10. If the School's response is judged to be inadequate, the enquirer should be alerted to the Complaints Procedure (GOVINF27).

Queen Elizabeth's School
DATA PROTECTION POLICY

LINKED POLICIES	❑ Code of Conduct for Staff and Governors ❑ Dealing with issues relating to Parental Responsibility ❑ Home-School Agreement ❑ ICT Policy ❑ Pupil Discipline Policy ❑ Safeguarding Policy ❑ Staff Disciplinary Procedure ❑ Staff Training and Development Policy ❑ Whistleblowing Policy
LINKED LEGISLATION AND REFERENCE MATERIALS	❑ Data Protection Act 1998 ❑ Data Protection Act 2018 ❑ Data Retention and Investigatory Powers Act 2014 ❑ Education Act (1996) ❑ Education (Independent School Standards) (England) Regulations 2010 [Part 6] ❑ Freedom of Information Act 2000 ❑ General Data Protection Regulation ❑ ICO guidance on GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ ❑ ICO Code of Practice for CCTV https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf ❑ ICO Subject Access Code of Practice https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf ❑ Information and Records Management Society toolkit https://irms.org.uk/page/schoolstoolkit?&terms=%22toolkit+and+schools%22 ❑ Protection of Freedoms Act 2012

Approved by the Governing Body on 31 October 2019

Signed .....

B.R. Martin, Chairman of the Governing Body