Loreto Grammar School

Data Protection Policy

Inception of policy	March 2018
Current policy approval date	January 2024
Next policy review date	January 2028
Distribution to	All staff
Owner of policy	Headteacher
Approved by	Staffing Governors' committee /Data Protection Governor
Reviewed and prepared by	Mrs Alford (DPO) and Ms Dugdale, Director of HR and Support Staff
Location of policy	HR Toolkit

Contents

1. Aims 4

2. Legislation and Guidance 4

3. Roles and Responsibilities 4

3.1 Specific Responsibilities 4
3.2 Governing Board 5
3.3 Data Protection Officer 5
3.4 Headteacher 5
3.5 All Staff 5
3.6 Additional Responsibilities of Staff 6
4. The Data Controller and Data Processor 6

5. Legal Obligations 7

5.1 Commitment to UK GDPR Principles and Accountability Rule 7
6. Data Collection 8

6.1 Lawfulness, Fairness and Transparency 8
6.2 Special Category Personal Data 8
6.3 Limitation, Minimisation and Accuracy 8
6.4 Consent 9
6.5 Responsibilities of Parents 9
6.6 Pupils 9
6.7 General Responsibilities of Employees in Respect of Their Own Data 9
6.8 Photographs and Videos 9
6.9 Biometric Recognition Systems 10
6.10 CCTV 10
7. Data Sharing 10

7.1 Disclosure Outside the EEA 11
7.2 Public Display of Employee Data 11
8. Data Security and Storage Of Records 11

8.1 Retention of Personal Data for Research and Archive Purposes 12
9. Disposal of Records 12

10. Data Breaches 12

11. Training 12

12. Data Subject Rights 12

12.1 Subject Access Requests 13
12.1.1 Children and Subject Access Requests 14
12.2 Responding To Subject Access Requests 14

12.3 Refusing Subject Access Requests 14
12.4 Other Data Protection Rights of The Individual 14
12.5 Parental Requests to See an Educational Record 15
12.6 Freedom of Information 15
13. New or Additional Processing 15
14. Data protection by design and default 15
15. Monitoring arrangements 16
Appendix A - Privacy Policies..... 17
Privacy Notice Parents 18
Privacy Notice School Workforce/Volunteers.....22
Privacy Notice Students..... 27
Appendix B - ICT Acceptable Use Policy - All Adults Working in School 32
Personal E-mail 33
Appendix C - Data Breach Procedure 34
Actions to minimise the impact of data breaches..... 35
Sensitive information being disclosed via email (including safeguarding records) 35
Appendix D – Subject Access Request 38
Appendix E – Freedom of Information Requests 42
Appendix F - Data Protection Definitions 43
A-Z Data Protection Terms..... 44

1. Aims

Our 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 Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), the Digital Economy Act 2017, the Human Rights Act 1998, the Freedom of Information Act 2000, and the Education Act. We also meet the requirements of the Protection of Freedoms Act 2012 in our use of biometric data. The Headteacher and Governors will act within the frameworks advised by the Information Commissioner's Office, Department for Education and the Local Education Authority.

This policy applies to all personal data, regardless of whether it is in paper or electronic format and irrespective of who the data subject is (be they employees, pupils or others). The information and guidelines in this policy apply to the whole Loreto community including staff, volunteers and pupils.

2. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO), the Information and Records Management Society (IRMS), Department for Education (DfE) and Diocese and follows the ICO's code of practice for subject access requests and the use of surveillance cameras. In addition, this policy complies with our funding agreement and articles of association.

The Headteacher and Governors are committed to providing and maintaining a data environment that is safe. The management of data risks is established by allocating specific duties to key staff and by producing additional policies and arrangements as detailed in this document. This will include the production of:

- Privacy Notices (Appendix A).
- Acceptable use of IT Policies for staff and students (Appendix B).
- Data Breach Procedure (Appendix C).
- Subject Access Procedures (Appendix D).
- Freedom of Information Procedures (Appendix E).
- Records Management and Retention Policies.
- A Record of Processing Activities.
- Other Information Security Policies as required.

This Policy sets out our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the school, its employees, agents, contractors, or other parties working on behalf of our school. All those involved in processing data are responsible for assisting us in the achievement of our aims and objectives and will play a positive role in promoting a secure data processing environment where the rights and freedoms of the individual are protected.

3. Roles and Responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 Specific Responsibilities

Specific data protection responsibilities are given to the following staff:

Area of Responsibility	Name	Role
Overall Responsibility for Data and Data Protection	Mrs Walker	Designated SLT Lead for Data Protection and IT Matters
Data Protection Governor	Mr J Hassall	Data Protection Governor
Data Protection Officer	Mrs S Alford	Main DPO
Internal Data Protection Officer and link to Main DPO	Ms Dugdale	Director of HR and Support Staff
Data and SIMS and FOI	Ms Wilcock	Data Manager
CPOMS	Mrs Green	Assistant Headteacher (Pupil Welfare) and DSL
Premises and Estates	Mr Beckett	Estates Manager
IT	Mr Lamb	IT and Network Manager
Staff with access to CCTV	Mr Beckett	Estates Manager
Staff with enhanced CPOMS access	Mrs Green	Assistant Headteacher (Pupil Welfare) and DSL
Staff with safeguarding responsibilities	Mrs Green Mr Newman Mrs Milton Mrs Lloyd-Davies	Safeguarding Team

3.2 Governing Board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

3.3 Data Protection Officer

The designated SLT lead for Data Protection and IT Matters is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The internal DPO is also the first point of contact for routine matters. Our Main DPO will provide advice, guidance and support for matters not of a routine nature.

Our Data Protection Officer (DPO) is Mrs Alford who is contactable by emailing the school on dpo@loretogrammar.co.uk

3.4 Headteacher

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

3.5 All Staff

It is the responsibility of every member of staff to maintain the quality of the data that the school processes and to comply with UK GDPR and the DPA 2018. Anyone who collects data, enters, extracts or analyses data on our Information Systems should be aware of how their job contributes to the school's function and

the need to ensure the safety and accuracy of the data that they process. Personal data processed by Loreto employees shall:

- Be kept for no longer than it is required for the purpose for which it was originally collected and thereafter securely disposed of.
- Be kept up to date and accurate as far as is reasonable.
- Be processed only where there is a lawful purpose.
- Not be used for purposes other than that for which it was collected (unless consent is obtained).

Any questions or concerns about the interpretation or operation of this policy should be taken up with the DPO.

Staff are responsible for:

- Collecting, storing and processing all personal data in accordance with this policy.
- Ensuring that any personal data, which they hold or process, is kept securely.
- Ensuring that personal data is not disclosed orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort is made to see that personal data is not disclosed accidentally.
- Informing the school of any changes to their own personal data, such as a change of address.
- Making sure that all third-party requests for access to personal data, including those from the police, are directed via the DPO.
- Contacting the DPO in the following circumstances:
    - If there has been a data breach.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they have any concerns that this policy is not being followed.
    - If they need help with any contracts or sharing personal data with third parties.
    - 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 EEA.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.

Staff should be particularly cognisant of how a lapse on their part could adversely affect our school's reputation, incur financial penalties from the ICO or affect performance or service delivery. In extreme circumstances lapses can have a negative impact on the allocation of funding to our school. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, access to school facilities being withdrawn, or even to a criminal prosecution. Unauthorised disclosure is a disciplinary matter. If in any doubt consult the Internal DPO or Mrs Walker.

3.6 Additional Responsibilities of Staff

In addition to their responsibilities as data users, all staff have additional responsibilities regarding the operation of this policy, which are:

- To inform the governors if they believe the Information Commissioner should be notified about any processing of personal data within the school.
- Obtain specific informed consent from data subjects where appropriate to process personal data (e.g. consent for marketing photography or to join the alumni association).
- Provide any personal data required t in response to a subject access or Freedom of Information request in a timely manner.
- Maintain the security of, and access to, personal data within their scope.

4. The Data Controller and Data Processor

Our school is both a "data controller" and "data processor" under the data protection regulations. This is because we determine the purpose and the means of processing of personal data as well as carrying out the processing itself on the personal data relating to parents, pupils, staff, governors, visitors and others. We also have a number of "sub-processors" (organisations who process data on our behalf) such as SIMS, CPOMS and Edulink. Our school is responsible for the actions of these "sub-processors". A complete list of our sub-processors can be obtained from the DPO.

Loreto Grammar School is registered with the ICO both as a data controller and a CCTV operator and renew our registration annually or as otherwise legally required. A copy of our registration is displayed in the School Office. Further details of this are available from Mrs Alford or Ms Dugdale or from the Information Commissioner's website at www.ico.gov.uk.

The UK GDPR and DPA 2018 aim to give control to individuals over their personal data and to put the rights and freedoms of individuals at the heart of data processing. As a processor of personal data our school will:

- Clearly disclose when data is collected.
- Declare the lawful basis and purpose for data processing.
- State how long data is being retained, if it is being shared (and who with), and how/when it will be disposed of.

Like all educational establishments, Loreto holds and processes information (personal data) about it's employees, applicants, pupils, alumni and other individuals (data subjects) for a variety of proposes such as the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll, and to enable correspondence and communications. Our school has a Legal Basis for processing each category of information and these are clearly articulated in our Privacy Policies and Notices (See Appendix A).

In this policy the term "personal data" describes any information that relates to an identified or identifiable living individual. This can be as simple as a name or a phone number or could include other factors such as pictures biometric information or voice recordings. If it is possible to identify an individual directly or indirectly from the information being processed then that information will be classed as personal data.

5. Legal Obligations

The school meets its legal obligations as laid down by the Data Protection Act 2018 by taking steps to establish appropriate retention periods for personal data and ensuring that data subjects' rights can be appropriately exercised. In addition to:

- Ensuring that all staff are made aware of good practice in data protection.
- Ensuring that everyone handling personal data knows where to find further guidance.
- Ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly.
- Implementing appropriate technical and organisational measures against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Providing adequate security measures to protect personal data.
- Providing adequate training for all staff responsible for personal data.
- Regularly reviewing data protection procedures and guidelines within the organisation.

5.1 Commitment to UK GDPR Principles and Accountability Rule

The UK GDPR is based on data protection principles that our school must comply with. Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. 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 in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data,

In addition to the six principals of processing (above) our school has developed a robust plan to demonstrate our compliance with the Accountability Rule of UK GDPR. We achieve this by regular Governor and SLT oversight of data protection matters, implementing appropriate policies and procedures, providing training for students and staff and conducting Data Audits and Data Protection Impact Assessments as necessary.

6. Data Collection

6.1 Lawfulness, Fairness and Transparency

All processing of personal data which is undertaken by data users in the course of their employment in our school must be in compliance with the principles above. The school will process personal data under the following legal reasons:

- **Consent**: the individual has given clear consent for us to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary in order to comply with the law (not including contractual obligations).
- **Vital interests**: the processing is necessary to protect someone's life.
- **Public task:** we consider that any processing required to provide a child with an education is a task in the public interest.
- **Legitimate interests:** we use this as our lawful basis where the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6.2 Special Category Personal Data

The school may from time to time process sensitive personal data such as medical data, ethnicity, religion and sex in relation to admissions applicants, pupils and employees of the school. This data will only be processed where the school has a Legal basis and a separate condition for processing special category data (e.g. vital interests).

6.3 Limitation, Minimisation and Accuracy

We only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals 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.

When staff, or the school, no longer require the personal data that they hold, they must ensure it is deleted or anonymised. This will be done in accordance with our school's Data Retention Schedule and Record of Processing Activities (which comply with the Information and Records Management Society's toolkit for schools and Academies).

6.4 Consent

Where our school relies on consent for processing this will be clearly articulated at the time of data collection. Consent will be requested on every occasion where the school wishes to use personal data for a reason other than that for which it was originally collected.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

6.5 Responsibilities of Parents

Parents must ensure that any personal data that they supply to the school is accurate and kept up- to-date. In particular, changes of address, telephone number, email address or other personal details should be provided to the school office as soon as possible. Parents are asked to review a hard copy of their child's record on an annual basis but may submit an update request to the Data Manager at any time if required.

6.6 Pupils

Pupils using Loreto computing facilities are required to comply with the data protection provisions and our computer use policy. (Appendix B1)

6.7 General Responsibilities of Employees in Respect of Their Own Data

All employees must ensure that any personal data that they supply to the school is accurate and up-to-date; and that the school is informed of any errors in, or changes to, information which they have provided, e.g. changes of address or marital status.

6.8 Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school. Where we don't need consent, we will clearly explain how the photograph and/or video will be used. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as our school photographer, newspapers, campaigns.
- Online on our school website or social media pages.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

6.9 Biometric Recognition Systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will obtain written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure 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, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

6.10 CCTV

We use CCTV in various locations around our school site for safeguarding and security reasons. We will adhere to the ICO's code of practice for the use of CCTV. Our CCTV is hosted on a standalone system and only named staff have access to the output of the cameras, the School's CCTV registration is displayed both in the school office and Estate Manager's office.

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 Mr Beckett, Estates Manager or to our DPO, Mrs Alford.

7. Data Sharing

We will not normally share personal data with anyone else, but may do so 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 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 we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
- We 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
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also 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.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

7.1 Disclosure outside the EEA

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing personal data. A decision will be made on a case by case basis for instances where individuals move to schools outside the EEA where no adequacy ruling exists and parents request a pupil's Educational Record be sent to the new school.

7.2 Public display of employee data

In order to assist with the proper functioning of our school, we may provide or publish employees' Loreto e-mail address, photograph and appropriate information about their school duties, whether in hard copy and electronic directories, upon enquiry, or on such websites as are approved by the school from time to time. Any objection to the provision of such details by the school in such circumstances should be provided to the Headteacher in writing.

8. Data security and storage of records

We will 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:

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- 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, pinned to notice/display boards, or left anywhere else where there is general access.
- 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 to change their passwords at regular intervals.
- 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 IT acceptable use policy).
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- 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.

8.1 Retention of Personal Data for Research and Archive Purposes

Despite the general requirement that data should be retained for no longer than is required, UK GDPR permits the retention of records for research and archival purposes. The Headteacher is responsible for the ultimate selection and preservation of records for archive and research purposes.

9. 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.

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.

10. 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 C.

When appropriate, the school is required to report a data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

11. 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. It will take place every 2 years at a minimum.

12. Data Subject Rights

UK GDPR gives rights to individuals in respect of personal data that an organisation holds about them. Data subjects have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Data Subject rights are:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

12.1 Subject Access Requests

An individual who wishes to make a "Subject Access Request" (SAR) to obtain a copy of the personal data that the school processes about them may submit their request to any member of staff in any format. If possible, individuals should be requested to complete the school “Subject Access Request Form” and send it to the Headteacher at head@loretogrammar.co.uk.

Subject access requests should include the name, contact details, address (email and correspondence) of the individual making the request together with details of the information requested. This information should be entered in the “Loreto Subject Access Request Log”. If the request is made verbally then the staff member to whom the request is made should take sufficient notes to answer the request. If possible, staff receiving the request should complete a “Loreto Subject
Access Request (Verbal)” data capture form and ensure that this is entered into the “Loreto Subject Access Request Log”.

On receipt of a Subject Access Request the school is required to respond within 30 days. Therefore, staff who receive a subject access request must immediately forward the matter to the DPO.

The information that will be provide under a subject access request will include an explanation of any internal codes contained within it. The data supplied will, in principle, be all that is held at the time that the request is made, although the law permits routine amendments and deletions of data to continue between the time of the request and the time of the reply. The school will not make a charge for such information.

The information that data subjects will receive includes:

- Confirmation that their personal data is being processed.
- A copy of the data (routinely provided as a hard copy).
- The purpose for which the data is processed (contained in our Privacy Documents).
- The categories of the personal data concerned (contained in our Privacy Documents).
- Who the data has been, or will be, shared with (contained in our Privacy Documents).
- How long the data will be stored for, or the criteria used to determine this period.
- The source of the data if it was not the individual making the request.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

The school’s Subject Access Request Guidance Document is attached to this Policy as Appendix D.

If the data subject has reason to believe that the school has not dealt correctly with their access request, the matter should be taken up in the first instance with the DPO. If the data subject is unsatisfied after discussion with the Data Protection Officer, they should contact the Information Commissioner who is officially appointed to consider such complaints. The address is: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Alternatively they may fill in the online form at https://ico.org.uk/make-a-complaint/.

12.1.1 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or to have given their consent.

Children 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 or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

12.1.2 Responding to Subject Access Requests

Prior to responding to requests, we:

- May ask the individual to provide 2 forms of identification (or identify themselves from information we hold about them).
- May contact the individual via phone to confirm the details of the request.

The school will:

- Provide the information free of charge.
- Respond without delay and within 1 month of receipt of the request - We 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:

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

12.1.3 Refusing Subject Access Requests

In accordance with the regulations the school reserves the right to reject repeated or vexatious requests where a reasonable period has not elapsed between requests and may charge for large volumes of documents. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

12.2 Other Data Protection Rights of The Individual

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

- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Be notified of a data breach (where there is a risk to their rights and freedoms).
- Challenge processing which has been justified on the basis of public interest.
- Make a complaint to the ICO.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them).
- Prevent processing that is likely to cause damage or distress.
- Prevent the use of their personal data for direct marketing.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Withdraw their consent to processing at any time (where consent is the basis).

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.

12.3 Parental requests to see an educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

As an Academy, Loreto is not obliged to answer such a request as there is no automatic parental right of access to the educational record. Each request will be considered on its own merit. Requests should be made in writing to the DPO.

12.4 Freedom of Information

The Freedom of Information Act 2000 establishes a general right of access to information held by public authorities. Loreto Grammar School abides by the act in two ways:

- We publish certain information about our activities proactively on our website.
- We respond to requests for information from members of the public.

The Act does not give people access to personal data, whether this is about themselves or others. If a member of the public wants to see information that we hold about them, they should make a "Subject Access Request".

The Loreto Grammar School Freedom of Information Policy is in appendix E of this policy.

13. New or Additional Processing

No employee may, without the prior written authorisation of the Headteacher /DPO:

- Develop a new computer system for processing personal data.
- Use an existing computer system to process personal data for a new purpose.
- Create a new manual filing system containing personal data.

- Use an existing manual filing system containing personal data for a new purpose.
- Create new folders on the main T/G drives file structure.

14. 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:

- Appointing a suitably qualified DPO, 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.
- 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).
- 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 make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Monitoring arrangements

The DPO is responsible for monitoring and recommending updates to this policy. Review of the policy will be undertaken by the Headteacher, Health and Safety/Premises Manager and the Resources Committee.

Appendix A - Privacy Notices

Privacy Notice Parents

Privacy Notice School Workforce/Volunteers

Privacy Notice Students

Loreto Grammar School
Privacy Notice for Parents

Loreto Grammar School collects pupil data and personal information in many forms and is the controller of such information. Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **parents**.

It is to help you understand how and why we collect personal information about you and what we do with that information. It also explains the decisions that you can make about this information.

We, Loreto Grammar School, are the 'data controller' for the purposes of data protection law. This means that the School determines the purposes for which and the manner in which personal data relating to parents and their families is processed

Our Data Protection Officer (DPO) is Mrs Alford who is contactable by emailing the school on dpo@loretogrammar.co.uk

What is Personal Information?

Personal information is information that identifies you as an individual and relates to you. This includes contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

Why does the School collect and use Personal Information?

Within the School we use pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to administer admissions waiting lists
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard pupils.

The categories of pupil information that we collect, hold and share about parents include:

- personal information (such as name, contact details and contact preferences)
- characteristics (such as ethnicity, language, nationality)
- CCTV images captured in school
- details of care packages, plans and support providers
- photographs
- safeguarding information

A complete up to date list of the data we collect about parents is available from our Data Protection Officer.

In some cases, data will be outsourced to a third-party processor. Where appropriate this will be done with your consent. Where the School outsources data to a third-party processor, they will be subject to the same data protection standards as Loreto Grammar School.

The Lawful Basis on which we use and process this information

We collect and use parent's information under the Education Act 1996 and the UK Data Protection Act 2018 (specifically the UK General Data Protection Regulations (UK GDPR) including Article 6 "Lawfulness of Processing" and Article 9 "processing of special categories of personal data. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest (education).

Less commonly, we may also process parents' personal data in situations where:

- We have obtained consent to use it in a certain way (e.g. photographs)
- We need to protect the individual's vital interests (or someone else's interests).

Some of the reasons listed above for collecting and using parents' personal data overlap, and there may be several grounds which justify our use of this data.

Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn. Please speak to the Headteacher if you would like to withdraw any consent previously given.

Legitimate Interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The School relies on legitimate interests for most of the ways in which it uses your information. Specifically, the School has a legitimate interest in:

- providing educational services to your daughter
- safeguarding and promoting the welfare of your daughter (and other children)
- promoting the objects and interests of the School. This includes fundraising. It also includes making sure that we are able to enforce our rights against you, for example, so that we can contact you if unpaid trip fees are due
- facilitating the efficient operation of the School; and
- ensuring that all relevant legal obligations of the School are complied with.

In addition, your personal information may be processed for the legitimate interests of others. If you object to us using your information where we are relying on our legitimate interests as explained above, please speak to the Headteacher.

Necessary for a Contract

We will need to use your information in order to perform our obligations under our contract with you. For example, we need your name and contact details so that we can update you on your daughter's progress and so that we can contact you if there is a concern.

Legal Obligation

Where the School needs to use your information in order to comply with a legal obligation, for example to report a concern to Children's Services. We may also be legally obliged to disclose your information to third parties such as the courts, the local authority or the police.

Vital Interests

For example, to prevent someone from being seriously harmed or killed.

Public Interest

We consider that we are acting in the public interest by providing education to your child.

Special Categories of Personal Information

The School must also comply with an additional condition where it processes special categories of personal information. These special categories for parents are information that reveals racial or ethnic origin, religious or philosophical beliefs,

- Substantial Public Interest - The processing is necessary for reasons of substantial public interest.
- Vital Interests - To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.
- Legal Claims - The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.
- Medical Purposes - This includes medical treatment and the management of healthcare services.

Collecting Parent Information

While the majority of information we collect about **parents** is mandatory, some information may be provided voluntarily. Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

Storing Parent Data

We hold your data for the duration of your daughter's time in the School thereafter the data that we no longer require will be deleted or destroyed. There are some circumstances in which we may need to keep your data beyond the date on which your daughter leaves the School for example some digital images may be retained until such time as we change our marketing material. In exceptional circumstances we may keep your information for a longer time than usual but we would only do so if we had a good reason and only if we are allowed to do so under data protection law. Our record retention schedule follows the guidance in the Information and Records Management Society's toolkit for schools. You can ask to see a copy of this by contacting the Data Protection Officer.

Who we Share Parent Information with

We occasionally share parent information with:

- our Local Authority
- the Department for Education (DfE)
- School Nurse
- Youth Support Services

Why we share Pupil Information

We do not share information about our parents with anyone without consent unless the law or our policies require us to do so.

Requesting Access to your Personal Data

Parents/carers can make a request with respect to their own data. If you make a subject access request, and if we do hold information about you or your child, we will:

- give you a description of it
- tell you why we are holding and processing it, and how long we will keep it for • explain where we got it from, if not from you or your child.

You also have the right to:
- object to processing of personal data
- prevent processing for the purpose of direct marketing
- have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

Where you exercise your rights under the data protection legislation will ask for proof of your identity before we can respond. We will do our utmost to respond within the required timescales and will keep you advised if there are any delays.

If a Parent, or those with parental responsibility, makes a Subject Access Request on behalf of a student and the pupil is in our second year or higher then the student will need to agree to the data to being released to the parent.

There are certain instances where your personal data will not be provided in a subject access request.

The right to be forgotten and the right to object to processing are not absolute rights as where there is a requirement in law for us to retain or process certain types of personal data we will continue to do so.

Educational records

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. Within Academies there is no automatic parental right of access to the educational record. Each request will be considered on its own merit. Requests should be made in writing to the Data Protection Officer.

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**:

Our Data Protection Officer (DPO) is Mrs Alford who is contactable by emailing the school on dpo@loretogrammar.co.uk

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

You can also write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel: 0303 123 1113

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Loreto Grammar School
Privacy Notice for School workforce/volunteers

Loreto Grammar School collects data and personal information about those employed to teach, volunteers, or those otherwise engaged to work at the School in many forms and is the controller of such information. This means that the School determines the purposes for which and the manner in which personal data relating to staff is processed.

In some cases, your data will be outsourced to a third party processor; however, this will only be done with your consent, unless the law requires the School to share your data. Where the School outsources data to a third party processor, they will be subject to the same data protection standards as Loreto Grammar School.

This policy is to help you understand how and why we collect personal information about you and what we do with that information. It also explains the decisions that you can make about your own information.

What is Personal Information?

Personal information is information that identifies you as an individual and relates to you. This includes your contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.
The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as title, full name, date of birth and national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group and nationality
- address information (such as your contact address to direct correspondence to and mobile and landline telephone numbers)
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- photographs (those taken for identification and for marketing)
- CCTV images (for safeguarding and security)
- qualifications (and, where relevant, subjects taught and languages spoken)
- medical information (such as food allergies or medication needed in an emergency)
- contact information for next of kin/emergency contact (someone you would want the School to contact in an emergency including their prefix, gender, name, telephone numbers and relationship to you)
- payroll information (such as bank account numbers for payment transfers)
- recruitment information such as right to work documents, references, CV and covering letters
- car registration number, make and colour if your car is to be parked on site
- disclosure and baring service information

We also process special categories of personal data that may include:

- physical or mental health needs
- racial or ethnic origin
- criminal convictions data
- civil and criminal proceedings, outcomes and sentences
- religious or other beliefs of a similar nature

This list is not exhaustive, to access the current list of categories of information we process please see our employee SIMs data sheet (available from Ms C Dugdale). More information on the systems we use are on the School data asset register and record of processing activities.

Why does the School collect and use Personal Information?

We use school workforce data to:

- enable you to be paid
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform our recruitment and retention policies
- facilitate safe recruitment as part of our safeguarding obligations
- permit better financial modelling and planning
- improve the management of our workforce
- comply with the law

The Lawful Basis on which we process this information

We collect and use staff information under the Education Act 1996 and the UK Data Protection Act 2018 (specifically the UK General Data Protection Regulations (UK GDPR) including Article 6 "Lawfulness of Processing" and Article 9 "processing of special categories of personal data. We process this information under the following categories:

Legitimate Interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The School relies on legitimate interests for many of the ways in which it uses your information. Specifically, the School has a legitimate interest in:

- Providing educational services;
- Safeguarding and promoting the welfare of children in our care
- Promoting the objects and interests of the School. This includes fundraising. It also includes making sure that we are able to enforce our rights against you
- Facilitating the efficient operation of the School
- Ensuring that all relevant legal obligations of the School are complied with.

In addition your personal information may be processed for the legitimate interests of others. If you object to us using your information where we are relying on our legitimate interests as explained above, please speak to the Headteacher.

N*ecessary for a Contract*

We will need to use your information in order to perform our obligations under our contract with you. For example, we need your name and contact details so that we can ensure that you are paid and that we can contact you in an emergency.

Legal Obligation

Where the School needs to use your information in order to comply with a legal obligation, for example to report a concern to the DfE. We may also have to disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.

Vital Interests

For example, to prevent someone from being seriously harmed or killed.

Public Interest

The School considers that it is acting in the public interest when providing education.

Special Categories of Personal Information

The School must also comply with an additional condition where it processes special categories of personal information. These special categories are: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (where freely given), genetic information and health information.

Substantial Public Interest

The processing is necessary for reasons of substantial public interest.

Vital Interests

To protect the vital interests of any person where that person cannot give consent, for example, if you are seriously hurt and are unconscious.

Legal Claims

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Medical Purposes

This includes medical treatment and the management of healthcare services.

We may ask for your consent to use your information in certain ways. If we ask for your consent to use your personal information you can take back this consent at any time. Any use of your information before you withdraw your consent remains valid. Please speak to the Headteacher if you would like to withdraw any consent given.

Storing this information

We hold school workforce data for the length of time you are employed by the School +10 years. Thereafter it is deleted or destroyed unless it relates to a safeguarding matter when it will be retained in accordance with our safeguarding policies.

Payroll and pensions data is kept for the duration of your time at the School +85 years in accordance with HMRC Regulations

Collecting workforce information

We collect personal information via initial applications and the staff data form.

Workforce data is essential for the school's/local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. We will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely on SIMS, on our servers or in hard copy files for a set amount of time. We list these times in our data retention schedule. More information on our data retention schedule and how we keep your data safe is in our Data Protection Policy and the staff handbook.

Who we share information with

We routinely share information with:

- our local authority
- the Department for Education (DfE)
- Ofsted
- your family in case of emergency
- commissioned providers of personnel and payroll services (Trafford)

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local Authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We are required to share information about our workforce members with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or wellbeing of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Requesting Access to your Personal Data

Under data protection legislation you have the right to request access to information that we hold about you. To make a request for your personal information contact our Data Protection Officer (details below) or the Headteacher (preferably in writing).

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

Where you exercise your rights under the data protection legislation and we need to do so we will ask for proof of your identity before we can respond. We will do our utmost to respond within the required timescales and will keep you advised if there are any delays.

There are certain instances where your personal data will not be provided in a subject access request. Particularly, in the staff context this will relate to copies of any references which have been given in confidence.

Your attention is drawn to the fact that the right to be forgotten and the right to object to processing are not an absolute right. There is a requirement in law for us to retain or process certain types of personal data in relation to our workforce.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

For more information about the DfE data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

Contact

If you would like to discuss anything in this privacy notice, please contact Ms Claire Dugdale who will liaise with the School 's Data Protection Officer if required, cdugdale@loretogrammar.co.uk.
To contact DfE: https://www.gov.uk/contact-dfe

Loreto Grammar School
Privacy Notice for students

Loreto Grammar School collects pupil data and personal information in many forms and is the controller of such information. Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **students**.

It is to help you understand how and why we collect personal information about your daughter and what we do with that information. It also explains the decisions that you/they can make about this own information.
We, Loreto Grammar School, are the 'data controller' for the purposes of data protection law. This means that the School determines the purposes for which and the manner in which personal data relating to pupils and their families is processed.

Our Data Protection Officer (DPO) is Mrs Alford who is contactable by emailing the school on dpo@loretogrammar.co.uk

What is Personal Information?

Personal information is information that identifies you as an individual and relates to you. This includes contact details, next of kin and financial information. We may also hold information such as your religion or ethnic group. CCTV, photos and video recordings of you are also personal information.

Why does the School collect and use Personal Information?
Within the School we use pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to administer admissions waiting lists
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard pupils.

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

- personal information (such as name, unique pupil number, date of birth, identification documents contact details and contact preferences)
- characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- assessment information and results of internal and external assessments and tests
- attendance information (such as sessions attended, number of absences and absence reasons)
- behavioural information
- CCTV images captured in school
- details of any medical conditions, including physical and mental health
- details of any support received, including care packages, plans and support providers
- exclusion information
- photographs

- post 16 learning information
- pupil and curricular records
- safeguarding information
- special educational needs information.

A complete up to date list of the data we collect about students is available from our Data Protection Officer.

In some cases, data will be outsourced to a third-party processor. Where appropriate this will be done with your consent. Where the School outsources data to a third-party processor, they will be subject to the same data protection standards as Loreto Grammar School.

The Lawful Basis on which we use and process this information

We collect and use pupil information under the Education Act 1996 and the UK Data Protection Act 2018 (specifically the UK General Data Protection Regulations (UK GDPR) including Article 6 "Lawfulness of Processing" and Article 9 "processing of special categories of personal data. We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest (education).

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way (e.g. biometrics)
- We need to protect the individual's vital interests (or someone else's interests).

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn. Please speak to the Headteacher if you would like to withdraw any consent given.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Legitimate Interests

This means that the processing is necessary for legitimate interests except where the processing is unfair to you. The School relies on legitimate interests for most of the ways in which it uses your information. Specifically, the School has a legitimate interest in:

- providing educational services to your daughter
- safeguarding and promoting the welfare of your daughter (and other children)
- promoting the objects and interests of the School. This includes fundraising. It also includes making sure that we are able to enforce our rights against you, for example, so that we can contact you if unpaid trip fees are due
- facilitating the efficient operation of the School; and
- ensuring that all relevant legal obligations of the School are complied with.

In addition, your personal information may be processed for the legitimate interests of others. If you object to us using your information where we are relying on our legitimate interests as explained above, please speak to the Headteacher.

Necessary for a Contract

We will need to use your information in order to perform our obligations under our contract with you. For example, we need your name and contact details so that we can update you on your daughter's progress and so that we can contact you if there is a concern.

Legal Obligation

Where the School needs to use your information in order to comply with a legal obligation, for example to report a concern to Children's Services. We may also have to disclose your information to third parties such as the courts, the local authority or the police where legally obliged to do so.

Vital Interests

For example, to prevent someone from being seriously harmed or killed.

Public Interest

The School considers that it is acting in the public interest when providing education to your daughter.

Special Categories of Personal Information

The School must also comply with an additional condition where it processes special categories of personal information. These special categories are: personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, biometric information, and health information.

Substantial Public Interest

The processing is necessary for reasons of substantial public interest.

Vital Interests

To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.

Legal Claims

The processing is necessary for the establishment, exercise or defence of legal claims. This allows us to share information with our legal advisors and insurers.

Medical Purposes

This includes medical treatment and the management of healthcare services.

Collecting Pupil Information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

Storing Pupil Data

We hold pupil data for the duration of your daughter's time in the School thereafter the data that we no longer require will be deleted or destroyed. There are some circumstances in which we may need to keep your data beyond the date on which your daughter leaves the School for example:

- we store individual copies of public exam results for the purpose of providing references or help replace lost certificates should your daughter require this information in later life
- we may also keep some information so that we can respond to future legitimate enquiries concerning your daughter's attendance at the School and digital images may be retained until such time as we change our marketing material.

In exceptional circumstances we may keep your information for a longer time than usual but we would only do so if we had a good reason and only if we are allowed to do so under data protection law. Our record retention schedule follows the guidance in the Information and Records Management Society's toolkit for schools. You can ask to see a copy of this by contacting the Data Protection Officer.

Who we Share Pupil Information with

We routinely share pupil information with:

- Schools, Schools and universities that the pupil's attend after leaving us
- our Local Authority
- the Department for Education (DfE)
- the NHS
- School Nurse
- Youth Support Services
- Careers Advisors.
- Active Learning Practice for School (ALPS)

Why we share Pupil Information

We do not share information about our pupils with anyone without consent unless the law or our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013.

Data Collection Requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools .

The National Pupil Database (NPD)

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census. Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards. The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supportinghttps://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-informationinformation . To contact DfE: https://www.gov.uk/contact-dfe.

Youth Support Services

Pupils aged 13+
Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19-year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers.

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

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19-year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers' advisers.
-

For more information about services for young people, please visit our local authority website.

Requesting Access to your Personal Data

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent. If you make a subject access request, and if we do hold information about you or your child, we will:

- give you a description of it
- tell you why we are holding and processing it, and how long we will keep it for
- explain where we got it from, if not from you or your child.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

If a Student does not make the Subject Access Request themselves and they are in our second year or later then the student will need to agree to the data to being released to a third party. Where a student exercises their rights under the data protection legislation and It is necessary we will ask for proof of their identity before we can respond. We will do our utmost to respond within the required timescales and will keep you advised if there are any delays.

There are certain instances where your personal data will not be provided in a subject access request. Particularly, in the student context this will relate to copies of any references which we have given in confidence.

The right to be forgotten and the right to object to processing are not absolute rights as where there is a requirement in law for us to retain or process certain types of personal data we will continue to do so.

Educational records

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. Within Academies there is no automatic parental right of access to the educational record. Each request will be considered on its own merit. Requests should be made in writing to the Data Protection Officer.

Contact

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **Data Protection Officer**: **Mrs Alford who is contactable by emailing the school on dpo@loretogrammar.co.uk**

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/ .

You can also write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel: 0303 123 1113

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Appendix B

ICT ACCEPTABLE USE POLICY

Adults working in School

All adults working with ICT equipment at Loreto Grammar School must ensure that they have read, and agree to abide by, the points below. As with all school policies it is rooted in the values of our Mission Statement which requires each of us to uphold honesty, justice and mutual respect.

School systems and equipment are provided for professional use, and the guidelines below apply to all use on school premises, elsewhere via e-mail or 'Remote Access', and when using material stored on external devices such as USB memory sticks/hard drives. School utilises Securus which identifies any misuse of school equipment or access to any unsuitable websites. All staff must read and comply with the Loreto Grammar School Data Protection Policy and Privacy Notice. In complying, they agree to the following:

Data Protection and Privacy

- The Headteacher may access the files of all other staff members in extreme circumstances (for example as part of a Subject Access Request Response). No files can be considered private.
- Do not give anyone access to your login name or password. Passwords should be changed regularly every three months and should conform to the recommended advice and format which will be shared by Mr Lamb.
- Staff planners and USB / electronic devices which are removed from the school site may only contain: (a) Resources in connection with a colleague's work. (b) Student data in the form of students' names, form groups, assessment data and school monitoring codes, as required for a colleague's work. No further personal information, including addresses and telephone numbers, photographs, personal identifiers and data relating to personal circumstances may be removed from the school site, such data should be retrieved from SIMS or any other data related software only when needed and used on the school site.
- Files and communications containing data other than in (b) above must be stored securely.
- USBs, or the files within them, which contain personal information must be password protected.
- When away from the school site it is the responsibility of the colleague to keep all personal data in planners or on USB devices safe.
- SIMS and any other data related software must not be visible on classroom screens when in use.
- SIMS and any other data related software must not be accessed off-site except for entry of assessment data and data for students' reports.
- No PC or laptop should be left unattended whilst logged on without being locked.
- Users should close their browser and log out when their session has finished.
- Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.
- Do not release personal details including phone numbers or personal e-mail addresses of any colleague or student.
- Do not use another person's login details or open other people's files without express permission.
- Do not corrupt, interfere with or destroy any other user's information.
- Do not attempt to visit sites which might be considered inappropriate, this includes any site including material relating to terrorism or extremism; all sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

- Storage space is at a premium. Do not store programs, videos, games, music etc. in your server space.
- Check before publishing student's work. From September 2023, parental permission will be sought for the sharing of work for new students. These consents will be stored in SIMS. For all other students, teachers should seek verbal consent from students before sharing work.
- All out of date personal data should be removed from school systems.
- Information that relates to a student must be anonymised or deleted once the student reaches 25 years old.
- The school can in no way be held responsible for loss of personal information from the network.
- When permitted to use your own device users should follow the school Bring Your Own Device (BYOD) guidance.

Internet

- Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.
- The Internet and Social Media sites should not be used for personal reasons during working hours.
- When using the Internet or e-mail in your classes with students:
- Remind students of the rules for using the Internet and e-mail.
- Watch for accidental access to inappropriate materials and report the offending site to Mr Lamb.

Personal E-mail/MS Teams

- Observe netiquette on all occasions. E-mail should not be considered a private medium of communication and could be subject to monitoring both internally and externally.
- Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal. Do not use language that could be calculated to incite hatred, against any ethnic, religious or other minority, or matters conflicting with equality rights.
- Make sure nothing in the messages could be interpreted as libellous.
- Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

You should report any breaches of the school's IT Code of Conduct to Mrs Walker. Data Protection breaches should be reported to Mrs Beever and Ms Dugdale (internal DPO) for advice.

Please sign below and copy. Keep one copy for your reference and return the other to HR for our records.

I confirm that I have read and agree to abide by the ICT Acceptable Use Policy of Loreto Grammar School.

Name: ……..

Signature: ……..

Date: ……..

NW/CD/P/POLICIES/2 SEPTEMBER 2023

Appendix C

Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO. A Flow Chart describing how we deal with Data Breaches at Loreto Grammar School is at the end of this appendix. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost.
    - Stolen.
    - Destroyed.
    - Altered.
    - Disclosed or made available where it should not have been.
    - Made available to unauthorised people.
- The DPO will enter the details of the breach into the "Breach Log" and then alert the Headteacher (and the chair of governors if appropriate).
- The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible after any breach.
- The DPO 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 DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO, taking further guidance if appropriate. This must be judged on a case-by-case basis. 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 (for example, key-coding).
    - Damage to reputation.
    - Loss of confidentiality.
    - 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 DPO must notify the ICO.

- The DPO will document all decisions in the Breach Log in case decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a protected area of the school network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. 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.
        - 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.
    - 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 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.
    - 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.
        - Description of the likely consequences of the personal data breach.
        - 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.
    - If the there is no risk to the rights and freedoms of individuals the DPO will annotate the breach log accordingly and consult with the Headteacher whether it is appropriate to advise the data subjects. All decisions will be taken by the Headteacher.
- 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.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause.
    - Effects.
    - 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 a protected area within the school network.

Actions to minimise the impact of data breaches

The school will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

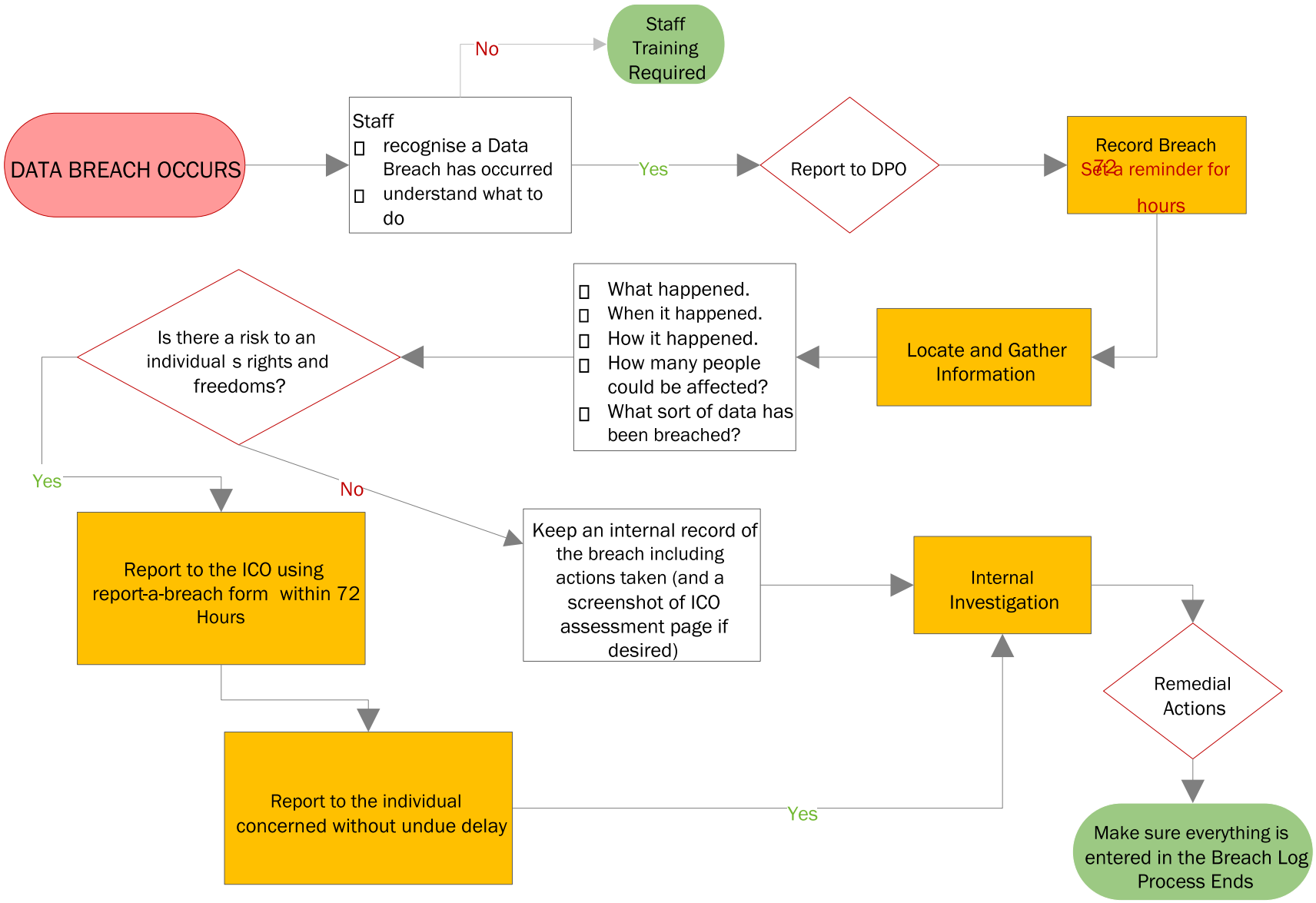
- If personal data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach that could occur:

- Non-anonymised pupil exam results or staff pay information being shared with governors.
- A self-access form reveals another user's data.
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked.
- The school's cashless payment provider being hacked and parents' financial details stolen.

Loreto Grammar School Data Breach Response Process



Appendix D

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 process is outlined in the flowchart at the end of this appendix. The rights of individuals 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 this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- Although we recognised that subject access requests may be made in any way. We request that subject access requests are submitted in writing, either by letter, email or fax to the DPO. In order to respond to a request in a timely manner requests should include:
- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

Any member of staff who receives a subject access request must immediately forward it to the DPO so that the information can be entered in the "Loreto Subject Access Request Log". If the request is made verbally then the staff member to whom the request is made should take sufficient notes to answer the request. If possible, staff receiving the request should complete a "Loreto Subject Access Request (Verbal)" data capture form and forward this to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or to have given their consent.

Children 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 or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Requests for large amounts of personal data

If we need more information before responding to a request, then we will let the individual know as soon as possible. The timescale for responding to the request begins when you receive the additional information. If an individual refuses to provide any additional information, we will still endeavour to comply with their original request.

Requests made on behalf of others

When a SAR is made via a third party such as a solicitor The school will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. The third party should provide us with evidence of this entitlement (either written authority or a more general power of attorney).

Processors and subject access requests

As Data Controller we are responsible for complying with a SAR. We will therefore ensure that we have contractual arrangements in place to guarantee that SARs are dealt with properly, irrespective of who they are sent to.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide up to 2 forms of identification or ask them to confirm 2 items of information that we hold about them.
- May contact the individual via phone to confirm what 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 student or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we 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. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Subject Access Responses

The information provided in any response will be concise, transparent, intelligible and in an easily accessible form, using clear and plain language. Any internal codes used in the source document will be explained. The school is not required to decipher poorly written notes or to ensure that that the information is provided in a form that can be understood by the individual making the request.

If data is regularly updated or altered it will be supplied as at the time of sending out a response, even if this is different to information which was held when the request was received. We recognise that it is an offence to make an amendment simply to prevent disclosure.

If possible or appropriate we will consider providing Data Subjects with remote access to a secure self-service system so that they can see all the personal information that is held on them (as long as this does not adversely affect the rights and freedoms of others).

Our SAR response will include:

- Confirmation that the school is processing the subject's personal data.
- A copy of all personal data as requested.
- Any other supplementary information about data processing activities (as set out in our privacy notice) which includes:
    - Our purpose for processing.
    - The categories of data we process.
    - Who we share/disclose the data with.
    - How long we store the data or, how we determine how long to store it.
    - Confirmation of their right of rectification, erasure or to restrict processing relevant to the situation (depending on your legal basis for processing).
    - Confirmation that they have a right to complain to the supervisory authority.
    - Information about the data source (if it is not themselves).
    - Information if automated decision-making takes place (including profiling).
    - Details of the safeguards we provide if we transfer personal data to a third country or international organisation.

What is NOT Included in a SAR Response?

An individual is not entitled to receive any information that relates to another person in a SAR response (unless they are acting on behalf of someone e.g. a Lawyer or Parent). Therefore, we will remove or redact any data which relates to other individuals. It is up to the school to decide if the information requested falls within the definition of personal data or not.

Recording SAR Requests

The DPO will make a record of the details of any SAR we receive in the SAR Log. Each request will be date stamped if necessary and saved in a specific folder for future reference.

Exemptions

In addition to the manifestly unfounded or excessive exemption there are several statutory exemptions contained in the DPA18. The majority of these exemptions relate to the detection and prevention of crime, national security and public functions such as immigration control.

Exemptions which relate to a commercial context including if the information:

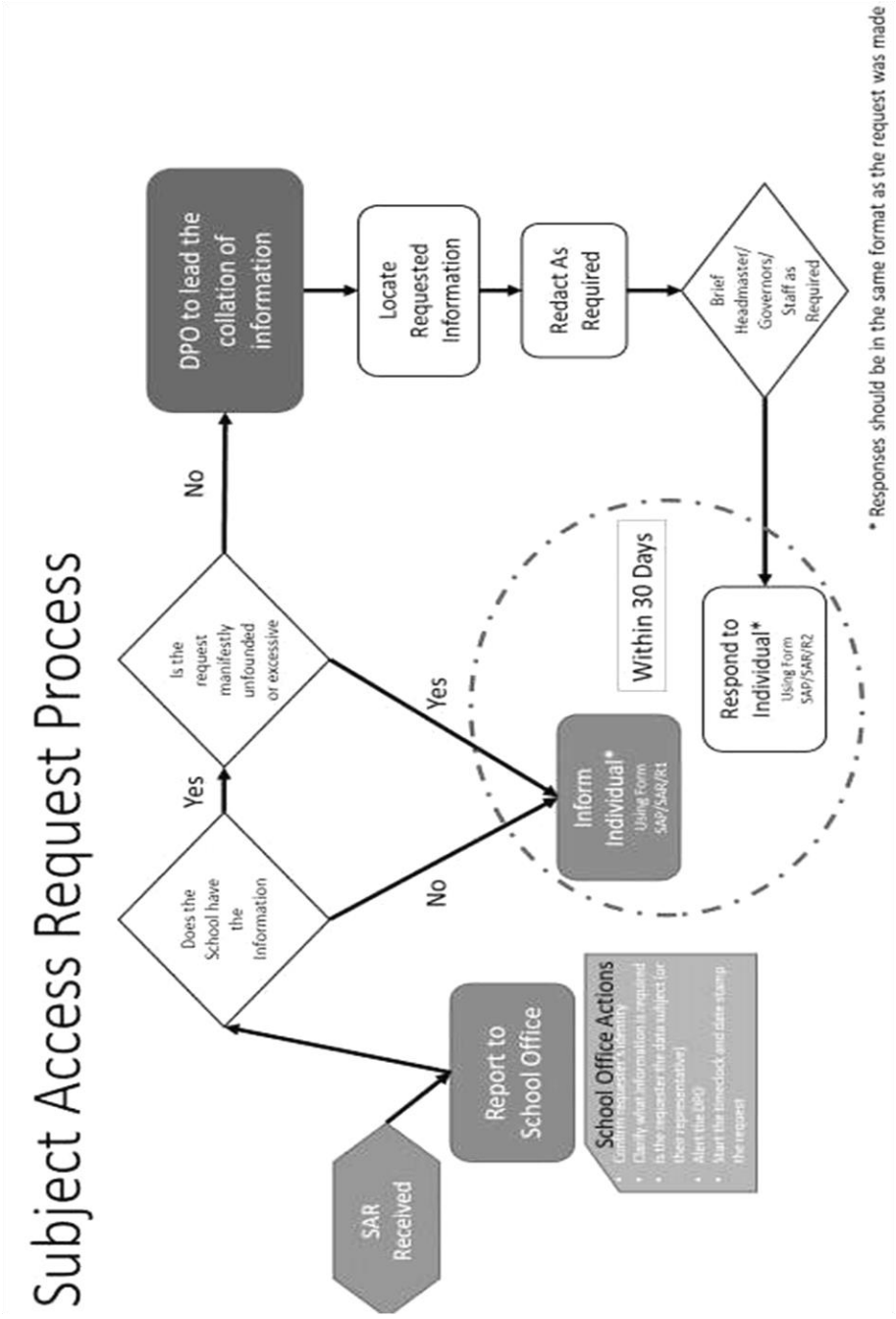
- is subject to legal or litigation privilege.
- is purely personal or for household use.
- is a reference for employment, training or educational purposes.
- is processed for management forecasting or planning in a business activity which could be prejudiced if it were to be disclosed.
- consists of records of intentions and relate to negotiations between the employer and employee and compliance with the request would prejudice the negotiations.
- contains a third party's personal data.
- is of the type which would be likely to prejudice crime prevention/detection or the prosecution of offenders if disclosed.

Information about a third party may only be disclosed where that person has consented to the disclosure or where it is reasonable to disclose the information without their consent. Therefore, the school will balance the rights of all the individuals involved taking into account:

- the type of information.
- any duty of confidentiality owed to the other individual.

- any steps we have taken to seek consent from the other individual.
- whether the other individual is capable of giving consent.
- any express refusal of consent by the other individual.

In a 'tie-breaker' situation, the presumption will fall in favour of non-disclosure.



Appendix E

Freedom of Information

The Freedom of Information Act 2000 establishes a general right of access to information held by public authorities, including academies. The school's Freedom of Information Policy and Publication Scheme is below. This policy should be used in conjunction with the latest ICO guidance on Freedom of Information (https://ico.org.uk/for-organisations/foi-eir-and-access-to-information/guide-to-freedom-of-information/).

Freedom of Information Policy & Publication Scheme

INTRODUCTION

The Freedom of Information Act 2000 ('the Act') was introduced to promote greater openness and accountability across the public sector and establishes a general right of access to information held by public authorities, including academies.

Loreto Grammar School ('the school') is responsible for compliance with the Act and will ensure that employees understand, and are able to comply with, requests for information under the Act.

The school is required by the Act to produce a publication scheme outlining its commitment to making information available to the public as part of its normal business activities, the different classes of information to be made available, the method by which this information will be made available and what charges can be made. The school's publication scheme can be found in section 6 of this policy.

SECTION 1 – FREEDOM OF INFORMATION REQUESTS

Freedom of Information requests must be made in writing, which includes email, include the enquirer's name, correspondence or email address and clearly describe the information requested. There must be sufficient information in the request to enable the school to identify and locate the information. The enquirer does not need to refer to the Act or provide an explanation as to why the information is required.

Requests under the Act should be made to Miss Julie Wilcock ('the Data Manager') at info@loretogrammar.co.uk.
Any requests addressed to any other member of staff must be passed to the Data Manager immediately upon receipt so that she can both acknowledge the request and deal with it in accordance with Section 2 of this policy. It is important to note that not all requests under the Act are standalone and may be contained within other communications about unrelated matters. Whenever there is a request for information, it should be referred to the Data Manager before any communication or acknowledgement is entered into with the enquirer.

If the request is ambiguous and/or the Data Manager requires further information in order to deal with it, she will request clarification and/or further information directly from the enquirer. The school is not obliged to deal with the request until the further information is received.

SECTION 2 - RESPONDING TO FREEDOM OF INFORMATION REQUESTS

Upon receipt of a request, the Data Manager will:-

- identify the information being requested;
- confirm or deny that the information requested is held by the school in recorded form;
- if held in recorded form;
    - confirm that a reply will be provided within the time for compliance;
    - obtain and collate the information;
    - prepare a draft response for approval, if necessary;
    - reply to the enquirer.

All email communications from the school will be sent from info@loretogrammar.co.uk. The Data Manager will retain a copy of each response and maintain a central record of each request, including;

- the source of the request;
- the subject matter of the request;
- the date the request was received;
- the date of the response.

The school is under a duty to respond to all requests, informing the enquirer whether or not the information is held, and supplying any information that is held, except where:

- absolute or qualified exemptions apply as provided for by the Act;
- the request is vexatious, that is, one which is designed to cause inconvenience, harassment or expense rather than to obtain information, and would require a substantial diversion of resources or would otherwise undermine the work of the school;
- there are repeated identical or substantially similar requests from the same enquirer unless a reasonable interval has elapsed between requests;
- the cost of compliance exceeds the threshold which is currently £450.

Where the information requested is already in the public domain either through the school's publication scheme or otherwise on the website, the school will direct the enquirer to the information and explain how to access it.

The school must respond to requests promptly and within the time for compliance which is the shorter of:

- 20 working days following the date of receipt, excluding any day that is not a school day;
- 60 working days following the date of receipt.

Where the school has asked the enquirer to provide more information to enable it to deal with the request, the time for compliance begins only when the further information has been received.

Where the school has notified the enquirer that a fee is to be paid, the time between the date the Fees Notice is given and the date payment is made will be disregarded from the calculation of the time for compliance.

SECTION 3 – DEALING WITH REQUESTS OUTSIDE OF THE FOIA PROCESS

In certain circumstances, it will be appropriate to deal with a request outside of the Freedom of Information Act process including:

- Where the information is readily available and can be provided quickly and easily in 'the normal course of business';
- Where the information requested is the enquirer's own personal data or his/her child's personal data. This will be dealt with as a Subject Access Request under the school's Data Protection Policy.
- Where the information requested is environmental information. This will be dealt with under Environmental Information Regulations.

SECTION 4 – FEES

The school may charge the enquirer a fee for providing the requested information. This will be dependent on whether the staffing costs in complying with the request exceeds the threshold, currently £450.

If a request would cost less than the threshold, the school may charge only for the cost of informing the enquirer whether the information is held and communicating the information to the enquirer (e.g. photocopying, printing and postage costs).

When calculating costs, the school can take account of the staff costs and time in determining whether the information is held by the school, locating and retrieving the information, and extracting the information from other documents. The school will not take account of the costs involved in considering whether information is exempt under the Act.

If a request would cost more than the threshold, the school can either refuse the request, answer and charge a fee, or answer and waive the fee.

If the school is going to charge it will send the enquirer a Fees Notice. The school does not have to comply with the request until the fee has been paid. More details on fees can be found on the Information Commissioner's Office ('ICO') website.

If the school intends to refuse a request for cost reasons, or charge a high fee, it will contact the enquirer in advance to discuss whether they would prefer the scope of the request to be modified so that, for example, it would cost less than the threshold.

Where two or more requests are made by different people who appear to be acting together or as part of a campaign, the estimated cost of complying with any of the requests may be taken to be the estimated total cost of complying with them all.

SECTION 5 – REFUSAL OF A REQUEST

If it is decided to refuse a request, the school will send a Refusal Notice, which must contain:

- the fact that the Data Manager cannot provide the information asked for;
- which exemption(s) apply;
- why the exemption(s) apply to this enquiry (if it is not self-evident);
- the reasons for refusal; and
- the school's complaints procedure.

For monitoring purposes and in case of an appeal against a decision not to release the information or an investigation by the ICO, the Data Manager must keep a record of all enquiries where all or part of the requested information is withheld and exemptions are claimed. The record must include the reasons for the decision to withhold the information.

SECTION 6 – PUBLICATION SCHEME

This publication scheme is based on the model publication scheme available from the ICO. It commits the school to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the school.

The scheme commits the school to:

- proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the school and falls within the classifications below;
- specify the information which is held by the school and falls within the classifications below;
- proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme;
- produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public;
- review and update on a regular basis the information the school makes available under this scheme;
- produce a schedule of any fees charged for access to information which is made proactively available;
- make this publication scheme available to the public;
- publish any dataset held by the school that has been requested, and any updated versions it holds, unless the school is satisfied that it is not appropriate to do so; publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the school is the only owner, make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the section 19 of the Act. The term 'dataset' is defined in section 11(5) of the Act. The term 'relevant copyright work' is defined in section 19(8) of the Act.

Classes of information

Who we are and what we do.
Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.
Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.
Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.
Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.
Current written protocols for delivering our functions and responsibilities.

Lists and registers.
Information held in registers required by law and other lists and registers relating to the functions of the school.

The services we offer.
Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.
- Information that is no longer readily available as it is contained in files that have been placed in archive storage or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available:

- The school will indicate clearly to the public what information is covered by this scheme and how it can be obtained.
- Where it is within the capability of the school, information will be provided on the website. Where it is impracticable to make information available on the website or when an individual does not wish to access the information by the website, the school will indicate how information can be obtained by other means and provide it by those means.
- In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.
- Information will be provided in the language in which it is held or in such other language that is legally required. Where the school is legally required to translate any information, it will do so.
- Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

Charges which may be made for information published under this scheme

- The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the school for routinely published material will be justified and transparent and kept to a minimum.
- Material which is published and accessed on the website will be provided free of charge.
- Charges may be made for information subject to a charging regime specified by Parliament.
- Charges may be made for actual disbursements incurred such as:
    - photocopying
    - postage and packaging
    - the costs directly incurred as a result of viewing information.
- Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.
- Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Act, or with other statutory powers of the public authority.
- If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Appendix F

Data Protection Definitions

Key Terms

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. At Loreto this includes the following: Name, Student Number, Tax Information, Address, Photograph, Online Identifier, Sexual Orientation, Location Data, Character Traits, Biographical Information, Current Living Situation, Email address, phone number, Location, Financial information, Educational Information, Private and Subjective Data, Sickness, Date of Birth, Appearance and Behaviour
Special categories of personal data	Personal data which is more sensitive needs more protection. At Loreto we process the following special categories of data: Racial/Ethnic Origin, Religious/Philosophical Views, Health, Genetic/Biometric Data, Criminal Record
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 living 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 (Loreto).
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.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

A-Z of Data Protection Terms

Term	Definition
Antivirus	Software to detect, stop and remove viruses/ malicious software from a system
Archive	A collection of information/records with a specific focus or theme (e.g. letters, documents, minutes, registers, maps, photographs, digital files, sound recordings)
Attacker	Someone who exploits computer systems in a malicious way
Biometric data	Personal data relating to physical, physiological or behavioural characteristics from which a person can be identified (e.g. fingerprints, images)
Botnet	A network of infected devices which are connected to the internet to commit coordinated cyber-attacks without their owner's knowledge
Brute force attack	When computer power is used to automatically send a vast number of requests or input a series of numbers in order to discover passwords and gain access to a system
Click farm	Where a large group of low paid workers are employed to click on advertising links in order to generate better results for the organisation being reviewed
Consent	Any freely given, specific, informed and unambiguous indication that the data subject agrees to an action (may be a statement or by clear affirmative action)
Cross border processing	Where personal data is processed by organisations in more than one Member State
Cyber attack	A malicious attempt to damage/disrupt/gain unauthorised access to computer systems/networks/devices by cyber means
Cyber incident	A breach of cyber security rules
Data minimisation	Where an organisation collects and keeps only the personal data it requires in order to achieve an intended purpose
Data Protection Authority	A national authority responsible for data privacy (the UK ICO)
Data protection by design and default	A principle whereby data subject's rights are taken into account at the design and development stage
Data protection impact assessment	A tool used to identify and minimise data protection risks in new projects
Data protection officer	An individual who is appointed to ensure an organisation implements and complies with the policies and procedures set out in the UK GDPR
Data transfer	The movement of personal data between organisations and people
Denial of service	When legitimate users are denied access to computer services or resources
Digital footprint	The 'footprint' of digital information that a user's online activity leaves behind
Download attack	The unintentional installation of malicious software or virus onto a device without the user's knowledge or consent

Encrypted data	Personal data which has been translated into another form or code so that only people with specific access can read it
Enterprise	A natural or legal person engaged in an economic activity, irrespective of its legal form (includes partnerships or associations)
EU-US privacy shield	A set of standards that allow for the legal transfer of personal data between the EU and US for commercial reasons
Fairness principle	The principle that requires personal data to only be used in a way that is fair and not detrimental, unexpected or misleading to the individuals concerned
Filing system	Any structured set of personal data, accessible according to specific criteria (may be centralised, decentralised or dispersed)
Firewall	Hardware or software which uses a defined rule set to constrain network traffic and prevent unauthorised access to/from a network
Group of undertakings	A controller and the group of undertakings or institutions affiliated to it
Hacker	Someone who uses their computer skills to break into computers, systems and networks
Health data	Personal data that relates to an individual's physical or mental health (including the provision of health care services)
Honeypot	A decoy system to attract potential attackers that helps limit access to actual systems
Information Society Service	Any service normally provided for remuneration, at a distance, by electronic means and at the request of a recipient (e.g. social media)
Integrity and confidentiality principle	A key requirement of UK GDPR for personal data to be processed using appropriate technical, organisational and security measures
International data transfer	The movement of personal data to countries outside the EU/EEA or to international organizations (this includes viewing data hosted in another location)
International organisation	An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries
Internet of things (iot)	Everyday objects such as televisions (not computers and devices) that connect to the Internet
Keylogger	Software that tracks keyboard inputs – used to monitor the user
Legal person	A human being, firm, or government agency that is recognized as having privileges and obligations
Legitimate interests	Where an organisation believes there is justification to process personal data because it will either benefit society as a whole or a particular company
Main establishment of the controller	The place, in the EU, where a data controller has their central administration or decision-making function
Main establishment of the processor	The place where a processing organisation's central administration or main processing activities take place
Malvertising	Using online advertising to deliver malware

Malware	Malicious software (viruses, trojans, worms or any code) that could have an adverse impact on organisations or individuals
Man-in-the-middle attack	Computer eavesdropping whereby an attacker secretly relays computer communications through themselves thus compromising the integrity or confidentiality of messages
Natural person	A living and breathing individual human being
Patching	Updates for firmware or software to improve security and/or enhance functionality
Pentest	An authorised test of a computer network or system designed to look for security weaknesses so that they can be fixed
Personal data	Any information relating to an identified or identifiable natural person who can be identified, directly or indirectly by some element of that data (e.g. name, identification number, location)
Pharming	An attack on a network that results in a user being redirected to an illegitimate website even though they entered the correct address
Phishing	Untargeted, mass emails asking for sensitive information (such as bank details) or directing them to a fake website or malicious link
Pii - Personally identifiable information	Information that can be used to identify, contact, or locate a single person, or to identify an individual either on its own or when combined with other information
Privacy impact assessment	A tool used to identify the privacy risk
Privacy notice	A document setting out (at the time of data collection) what data will be collected, the organisation's purpose and legal basis for processing the data, the subject's rights, how long the data is retained, who it will be shared with and how it will be disposed of
Profiling	Any form of automated processing which uses that data to evaluate certain personal aspects. In particular, where it is used to analyse or predict aspects of that person's performance or movements
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information (e.g. a key)
Purpose limitation	The principle that information may only be used for the specified, explicit and legitimate purpose for which it was collected and not for any other purpose
Pwned	A notification that an account's defences have been compromised
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Recipient	A natural or legal person, public authority, agency or another body, to whom personal data is disclosed
Relevant and reasoned objection	An objection to a draft decision by a supervisory authority or opinion that an envisaged action by a controller or processor does not comply with this Regulation
Representative	A person within the EU who is chosen or appointed to act or speak for a controller or processor who is based outside the EU

Sanitisation	Electronic or physical destruction methods to securely erase or remove data from memory
Smishing	Phishing via SMS text
Software as a service (Saas)	A business model where consumers access centrally-hosted software applications over the internet
Spear-Phishing	A targeted form of phishing, where the email is designed to look like it comes from a person the recipient knows and/or trusts
Spoofing	Faking (or imitating) a sending address to get access to a system
Subject access	The right of the subject to obtain or request certain information relating to their personal data from a data controller
Third party	An organisation or person (other than the data subject, controller, processor) who has been authorised to process personal data by the Data Controller/Processor
Trojan	A malware or virus disguised as legitimate software and used to hack into the victim's computer
Two-factor authentication	The use of two different components to verify a user's identity
Water-holing	A fake website (or a compromised real one) which exploits visiting users
Whaling	Highly targeted phishing attack (masquerading as a legitimate emails) aimed at or purporting to come from senior executives
Whitelisting	A list of approved applications or addressees in an organisation which protects systems from potentially harmful applications