Loreto Grammar School

Data Protection Policy (Examinations)

2026/2027

This policy is reviewed annually to ensure compliance with current regulations and reflects centre practice

Approved/reviewed by	
Mrs Stokes	
Date of next review	October 2027

Key staff involved in the policy

Role	Name(s)
Head of centre	**Mrs Beever**
Exams officer	**Miss McAulay**
Senior leader(s)	**Mrs Walker, Mrs Stokes, Ms Greene**
IT manager	**Mr Lamb**
SIMS manager	**Miss Wilcock**

Purpose of the policy

This policy details how Loreto Grammar School, in relation to the management and administration of examinations and assessments, will handle personal data in accordance with applicable UK data protection legislation and the requirements of the Joint Council for Qualifications (JCQ).

The delivery of examinations and assessments involve centres and awarding bodies processing a significant amount of personal data, including information relating to candidates, staff, examiners, assessors and other individuals involved in the examination process. Personal data is information relating to an identified or identifiable living individual.

Loreto Grammar School ensures that personal data is processed in accordance with the **UK General Data Protection Regulation (UK GDPR)**, the **Data Protection Act 2018 (DPA 2018)**, as amended by the **Data (Use and Access) Act 2025 (DUAA)**, and any other applicable data protection legislation, regulatory requirements and statutory codes of practice. The centre must also comply with any applicable requirements relating to the processing of personal data in other jurisdictions where relevant. The DUAA has amended, but does not replace, the UK GDPR and the DPA 2018.

JCQ's **General Regulations for Approved Centres** (section 6.1) require centres and awarding bodies to comply with current data protection legislation. JCQ's reference to 'data protection legislation' includes the UK GDPR, the DPA 2018 and relevant statutory codes of practice issued by the Information Commissioner. JCQ also requires centres to ensure that candidates are properly informed when their personal data is transferred to awarding bodies.

Relevant staff Loreto Grammar School ensure that they assume responsibility for ensuring that candidates are provided with appropriate privacy information about how their personal data is collected, used and shared. This includes explaining, where applicable, that relevant personal data such as a candidate's name, date of birth, gender and other information required for the administration, assessment and awarding of qualifications may be provided to awarding bodies.

All exams office staff and other individuals who collect, access, use, store or share personal data must follow the centre's data protection procedures and the **seven data protection principles** set out in Article 5 of the UK GDPR. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not processed in a way that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept in a form that permits identification of individuals for no longer than is necessary;
- processed using appropriate technical and organisational measures to ensure security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- processed in accordance with the principle of accountability, meaning that the centre must be responsible for, and able to demonstrate, compliance with the data protection principles.

Where exams office staff at Loreto Grammar School process **special category data**, such as information concerning a candidate's health or disability where this falls within the definition of special category data, or other particularly sensitive information, they are aware that an appropriate condition for processing must also be identified in accordance with applicable legislation.

This policy applies to personal data processed as part of the management and administration of examinations and assessments, regardless of whether the information is held electronically, in paper records or in another format.

Loreto Grammar School will also apply appropriate confidentiality and information-security measures to examination-related information that may not itself constitute personal data, particularly where disclosure, loss, alteration or unauthorised access could compromise the security or integrity of examinations and assessments.

Section 1 – Exams-related information

There is a requirement for the exams office(r) to hold exams-related information on candidates taking external examinations. For further details on the type of information held please refer to Section 5 below.

Candidates' exams-related data may be shared with the following organisations:

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- Department for Education; Trafford Local Authority; Diocese of Shrewsbury; relevant press agencies

This data may be shared via one or more of the following methods:

- hard copy
- email
- secure extranet site(s) – e.g. AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website
- A MIS provided by Capita SIMS sending/receiving information via electronic data interchange (EDI) using the data transport application or by integrated data transfer (www.jcq.org.uk/exams-office/data-transport-application/) to/from awarding body processing systems

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post-results/certificate information.

Section 2 – Informing candidates of the information held

Loreto Grammar School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via email
- given access to this policy via the school website

Candidates are made aware of the above, where candidates are following GCE and GCSE qualifications, when the entries are submitted to awarding bodies for processing.

Student Materials

Materials which are submitted by candidates for assessment may include any form of written work, audio and visual materials, computer programmes and data ("Student Materials"). Candidates will be directed to the relevant awarding body's privacy notice if they require further information about how their Student Materials may be used by the awarding body.

Candidates are informed that:

- by submitting Student Materials for assessment, the awarding body is entitled to use those Student Materials to the extent necessary to give effect to the assessment, qualification and regulatory framework, as set out in sections 6.17-6.19 of JCQ's *General Regulations for Approved Centres* document
- they are not entitled to opt-out of allowing awarding bodies to use these materials for the purposes set out in sections 6.17-6.19
- the awarding body will anonymise materials used for teacher and examiner training, inclusion in examiner reports and similar assessment-related publications and research directly related to the awarding body's assessment, qualification and regulatory activities
- they may notify the awarding body, by giving notice to the exams manager/officer or a member of senior leadership at Loreto Grammar School that they wish to opt out of the awarding body's use of their materials for teacher and examiner training, inclusion in examiner reports and similar assessment-related publications and research directly related to the awarding body's assessment, qualification and regulatory activities. Relevant staff will submit promptly to the relevant awarding body any notice received from a candidate

Access Arrangements

Candidates eligible for access arrangements which require awarding body approval using *Access arrangements online* are informed that an application for access arrangements will be processed using *Access arrangements online*, complying with the UK GDPR and the Data Protection Act 2018.

Malpractice

Candidates involved in suspected or alleged malpractice will be informed that their personal data will be provided to the awarding body (or bodies) whose examinations/assessments are involved, and that personal data about them may also be shared with other awarding bodies, the qualifications regulator or professional bodies, in accordance with the JCQ document *Suspected Malpractice – Policies and Procedures*.

Candidates reported for suspected or actual malpractice where a joint investigation by more than one awarding organisation is to be conducted, will be informed that awarding organisations will be responsible for ensuring that any sharing of data between awarding organisations is carried out in line with their statutory obligations under data protection legislation (primarily the Data Protection Act 2018 and UK GDPR).

Personal data

Candidates will be informed:

- that awarding bodies may be required to provide a candidate's personal data to educational agencies, such as DfE, Welsh Government, Department of Education (Northern Ireland), ESFA, regulators, HESA, UCAS, Local Authorities and the Learning Records Service (LRS)
- that their personal data may be provided to a central record of qualifications approved by the awarding bodies for statistical and policy development purposes

- of the processing that the centre undertakes, for example, that the centre will provide relevant personal data, including name, date of birth and gender, to the awarding bodies for the purpose of examining and awarding qualifications

Candidates may obtain access to their personal data, such as examination results by applying to the appropriate awarding body's data protection officer.

Candidates are also referred to the centre's privacy notice which explains:

- why Loreto Grammar School needs to collect personal data
- what it plans to do with it
- how long it will keep it
- whether it will be sharing it with any other organisation

Section 3 – Hardware and software

Technical security features, such as anti-virus software, are kept up-to-date and managed by the Network Manager and IT technicians. Firewalls are switched on at all times. Staff and students are advised not to download unapproved software or open unfamiliar email attachments. Staff members and students are advised to report all malware and virus attacks to IT technicians.

All members of staff and students have their own unique usernames and private passwords to access the school's systems and are responsible for keeping them private at all times. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are not in use. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

Access to and the use of emails is managed in line with the IT Acceptable Use Policy. Staff and students are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Personal email accounts are not permitted to be used on the school site.

Any email that contains sensitive or personal information is only sent using secure or passworded/encrypted email. The school's monitoring system can detect inappropriate links, malware and profanity within emails; staff and students are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

The table below sets out the measures in place to protect IT hardware, software and access to online systems used for the management and administration of examinations and assessments, supporting compliance with applicable UK data protection legislation and information security requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Laptops – various models	All purchased or acquired 2020-25 year	12 months
Desktops – Stone/Converge	All classroom pcs 4 months old. Staffroom pcs 3 years old	12 months

Software/online system	Protection measure(s)	Further details
OS system software - Windows 11 Edu - 26H2 – the latest version. We use the latest Sophos XG Firewall and Sophos endpoint with Interceptx on all IT equipment hosted on Sophos Central. Application software dependant on requirement. Microsoft Office365 being our main day to day application	We are a Windows AD Domain on Windows Server 2016 up to 2025. All accounts used in the process of exams are controlled accounts created by IT Services. Various permissions are set at account level dependent on the need of the exam requirements. MF authentication is used on key school accounts	Only IT services personnel have access to AD Domain Users and Computers – 2 staff members – IT manager and IT technician.
All school computers are built using our image delivery systems. PDQ deploy and Windows Deployment services WDS. *We use ExamWritePad for all written exams when using a laptop or PC.* *ExamWritePad backs up to a secure private location every 60 seconds.*	Complex passwords are set for all school accounts. As for exam accounts only IT Services staff have access to these.	Computers setup for exams are monitored by IT Services at all times, OR until the exam invigilator is present in the room. Backup of school data is the 3-2-1 methodology with all server data backed up onsite and to the cloud.
SIMS	Secure accounts for staff. SIMS permissions regularly reviewed by our GDPR officer for accuracy and specific need of the staff member	Updated in line with SIMS update services.
Edulink	Secure accounts for staff, students and Parents. Exam results and parent teacher feedback	Data kept relevant from SIMS database

Section 4 – Dealing with data breaches

Although personal data is handled in accordance with applicable UK data protection legislation and the centre's information-security procedures, a personal data breach may occur. A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data. A breach can therefore affect the confidentiality, integrity or availability of personal data.

A personal data breach may occur for a number of reasons, including:

- loss or theft of personal data or equipment on which personal data is stored
- inappropriate or inadequate access controls resulting in unauthorised access or use
- equipment or system failure resulting in the loss, alteration or unavailability of personal data
- human error, such as sending personal data to the wrong recipient or accidentally disclosing information
- unforeseen circumstances, such as fire, flood or other events affecting the availability or security of personal data
- unauthorised access resulting from hacking, phishing or other cyber-attacks
- obtaining personal information by deception, including 'blagging' or social-engineering techniques
- malware or ransomware attacks that result in personal data being accessed, altered, lost or made unavailable

A personal data breach may be accidental or deliberate. Not every security incident will require notification to the Information Commissioner's Office (ICO), but all personal data breaches must be recorded and assessed to determine the appropriate response.

If a personal data breach is identified or suspected, the following steps will be taken.

1. **Containment and recovery**

Mrs Walker (Deputy Headteacher) will lead, or coordinate, the centre's response to the breach.

Immediate action will be taken to contain the breach and prevent further loss, unauthorised access, disclosure or damage. This may include:

- identifying who needs to be informed and what action they are required to take
- isolating or disabling a compromised device, account, system or section of the network
- changing passwords, access credentials or permissions where necessary
- locating and securing lost or stolen equipment or physical records
- recalling or securely deleting information that has been sent or disclosed in error, where this is possible
- restoring personal data from secure backups where data has been lost, damaged or made unavailable
- taking steps to prevent compromised accounts or stolen information from being used to gain further unauthorised access; and
- obtaining assistance from the centre's IT provider, data protection lead, data protection officer, awarding bodies or other relevant organisations where appropriate

The centre will also determine whether any third parties, including data processors, need to be contacted. Where a processor experiences a personal data breach, it must inform the centre without undue delay so that the centre can assess and fulfil its own data protection obligations

2. Assessment of ongoing risk

The centre will promptly assess the likelihood and severity of the potential adverse effects of the breach on the rights and freedoms of individuals.

The assessment will consider, as appropriate:

- what categories of personal data are involved
- whether any special category data or other particularly sensitive information is involved
- how sensitive or confidential the information is
- the number of individuals affected and the approximate number of records involved
- the nature of the breach, including whether personal data has been lost, destroyed, altered, accessed or disclosed without authorisation
- who may have accessed or received the information and whether they are known and trusted;
- whether appropriate security measures, such as encryption, were in place
- whether the personal data remains accessible, usable and secure
- the potential consequences for the individuals concerned, including risks of identity theft, fraud, discrimination, financial loss, distress, reputational damage or loss of confidentiality
- the characteristics of the individuals affected, including whether children or other potentially vulnerable individuals are involved
- the likelihood that harm could occur and the severity of any potential harm; and
- the effectiveness of any measures already taken to contain the breach or reduce the risk

The primary consideration when assessing risk will be the potential impact on the individuals whose personal data has been affected. The centre will document its assessment and the reasons for the actions and decisions taken.

3. Notification and reporting

Following the risk assessment, Mrs Walker will determine whether the breach must be reported to the ICO and/or the individuals affected.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the centre will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If notification is made after 72 hours, the centre will provide the ICO with reasons for the delay.

Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the centre will also inform the affected individuals without undue delay, unless an exception under applicable data protection legislation applies. The communication will explain, in clear and plain language, the nature of the breach, the likely consequences and the measures taken or proposed to address the breach and mitigate its effects. Where appropriate, individuals will also be given advice on steps they can take to protect themselves.

The centre will keep a record of all personal data breaches, including those that do not require notification to the ICO or affected individuals. The record will include the facts relating to the breach, its effects and the remedial action taken.

4. Investigation, evaluation and improvement

Once the immediate response to the breach has been completed, the centre will review the incident to identify its cause and determine whether further action is required.

The review may include:

- reviewing what personal data was involved and where and how it was stored
- identifying weaknesses or vulnerabilities in technical and organisational security measures
- reviewing access controls, passwords, permissions and authentication arrangements
- reviewing methods used to share, transfer and transmit personal data
- reviewing the use of portable storage devices, personal devices and public or unsecured networks
- considering whether relevant data protection policies and procedures were followed
- reviewing whether staff had received appropriate training and guidance
- providing additional training, advice or supervision where necessary
- reviewing contracts and arrangements with relevant data processors or other third parties
- reviewing and, where necessary, updating contingency, backup and business-continuity arrangements; and
- implementing measures to reduce the likelihood or impact of a similar breach occurring in the future

The outcome of the investigation and any actions arising from it will be documented in accordance with the centre's accountability and record-keeping requirements.

Section 5 – Candidate information, audit and protection measures

For the purposes of this policy, personal data relating to candidates and other individuals involved in examinations and assessments will be processed in accordance with applicable UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025 (DUAA), and relevant regulatory guidance.

The centre will apply appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, alteration or damage. The measures applied will be proportionate to the nature and sensitivity of the information and the risks associated with its processing.

Examination-related information that does not constitute personal data will also be subject to appropriate confidentiality, security and examination-security controls where its loss, disclosure, alteration or unauthorised access could compromise the integrity or security of examinations or assessments.

The centre will maintain an information audit or appropriate record of processing activities to identify the categories of examination-related personal data held, the purposes for which it is processed, where it is held, who has access to it, how it is protected and, where

applicable, how long it is retained. The audit will be reviewed [insert frequency, e.g. annually] and whenever there is a significant change to the centre's examination processes, systems, suppliers or information-security arrangements. This supports the centre's accountability obligations and its ability to demonstrate compliance with data protection requirements.

The table in section 8 details the types of candidate examination-related information held by the centre and how that information is managed, stored, accessed, retained and protected.

Protection measures

Depending on the nature and risk associated with the information, appropriate protection measures may include:

- access to systems and files restricted to authorised staff with a legitimate need to access the information
- password-protected accounts and systems, using appropriate authentication and access controls
- secure network drives, databases or other approved storage locations with access restricted according to staff roles and responsibilities
- appropriate physical security for paper records, examination materials and IT equipment
- encryption or other appropriate security measures for personal data stored on or transferred using portable devices or other media
- secure methods for sharing or transmitting personal data, particularly where sensitive or confidential information is involved
- appropriate backup, recovery and business-continuity arrangements to protect the availability and integrity of personal data
- up-to-date operating systems, software, web browsers, anti-malware protection, firewalls and other security controls, in accordance with the centre's IT security arrangements
- regular review and testing of security measures to ensure that they remain appropriate to the risks presented by the processing
- secure disposal or deletion of personal data when it is no longer required to be retained
- appropriate staff training, guidance and procedures to reduce the risk of accidental or unauthorised disclosure, loss or misuse of personal data.

Technical and organisational measures at Loreto Grammar School are regularly reviewed and appropriate changes made where risks, technology, examination processes or legal and regulatory requirements change.

Section 6 – Data retention periods

Details of retention periods, the actions taken at the end of the retention period and method of disposal are contained in the centre's Archive Policy, which is available on the website.

Section 7 – Access to information

Under UK data protection legislation, individuals have the right to obtain a copy of their personal data and information about how their personal data is being processed. This is commonly known as the right of access or a subject access request (SAR).

In relation to examinations and assessments, a candidate may, depending on the circumstances, request access to personal data contained in examination-related records. This may include:

- their examination marks or results, where these constitute their personal data
- personal data contained in comments or annotations made by an examiner or assessor; and
- personal data contained in records relating to an examination appeal or review

The right of access does not automatically provide a candidate with a copy of their completed examination script or answers. Examination scripts are subject to specific provisions under UK data protection legislation, and whether a script is considered the candidate's personal data will depend on the circumstances. The centre will therefore consider requests for examination scripts in accordance with the applicable legislation and relevant ICO guidance. ICO – Exam results and your personal information

Requesting examination information

Requests for access to personal data or examination-related information should be made to Miss Wilcock, Data Manager, using the info@loretogrammar.co.uk email address

A request does not have to refer specifically to the UK GDPR or use the term 'subject access request' to be valid. Staff receiving a request that may constitute a subject access request will promptly refer it to Miss Wilcock in accordance with the centre's data protection procedures.

The centre may request information reasonably necessary to confirm the identity of the person making the request where there is a reasonable basis for doing so. This is particularly important where the requester is a former candidate or is not known to current centre staff.

Requests made by children

Children have data protection rights in their own right. There is no fixed age at which a child automatically acquires the right to make a subject access request. The centre will consider whether the child is able to understand what they are requesting and the implications of the request.

As a general guide, the ICO considers that a child aged 12 or over is generally presumed to have sufficient maturity to exercise their data protection rights, although this should not be treated as an absolute rule. A younger child may be sufficiently mature to exercise their rights, while an older child may require additional support.

Each request will therefore be considered on its individual circumstances, taking into account the child's maturity and understanding and, where appropriate, their wishes regarding the involvement of a parent or person with parental responsibility.

Where a parent, guardian or other person makes a request on behalf of a child, the centre will consider whether the person making the request is authorised to act on the child's behalf and whether it is appropriate to provide the requested information. The child's best interests and the child's own wishes, where they can be established, will be taken into account. ICO – Children's data protection rights

A decision regarding whether a child has sufficient understanding to make a request independently will be made by Ms Greene, Assistant Headteacher, in consultation with the centre's Data Protection Officer or other appropriate person where necessary.

Responding to subject access requests

The centre will normally respond to a valid subject access request without undue delay and within one calendar month of receiving the request or within one month of receiving any

information reasonably required to confirm the requester's identity or authority to act on behalf of the individual.

Where a request is complex or a number of requests have been made by the same individual, the response period may be extended by up to two further months where permitted by UK data protection legislation. The individual will be informed within the initial one-month period if an extension is required and given an explanation of the reasons for the delay.

The applicable time period will begin once the centre has received the request and any information reasonably required to confirm the requester's identity.

Where a request relates to examination information and specific statutory provisions or exemptions apply, the centre will consider those provisions when determining what information can be disclosed and when it must be provided. The centre will liaise with the relevant awarding organisation where appropriate.

Third-party requests and disclosure

Personal data relating to one individual will not normally be disclosed to another individual or organisation unless there is a lawful basis for doing so and the disclosure is otherwise permitted under applicable data protection legislation.

Where a third-party requests personal data on behalf of a candidate, the centre may require appropriate evidence that the candidate has authorised the third party to act on their behalf. The centre may also require sufficient information to verify the identities of the candidate and the third party.

Where a third party has a legal authority or other lawful basis to request information, the centre will consider the request in accordance with that authority and applicable data protection legislation. Consent is not necessarily the appropriate legal basis in every circumstance.

In the case of looked-after children or children in care, information may be shared with a local authority or other relevant organisation where there is an appropriate lawful basis and the disclosure is necessary and proportionate. Existing information-sharing agreements or statutory duties will be considered as appropriate. Any request that raises uncertainty about the lawful basis for disclosure will be referred to Ms Alford before information is released.

The centre will keep an appropriate record of significant decisions relating to requests for access to or disclosure of personal data, including the reasons for refusing or limiting disclosure where applicable.

Sharing information with parents and other persons

The centre will consider all relevant legal requirements and official guidance when deciding whether examination-related information may be shared with a parent, person with parental responsibility, non-resident parent, local authority or other third party.

Data protection legislation does not, by itself, determine whether a parent is entitled to receive information about their child. The centre will also consider relevant education law, the legal status and rights of the person requesting the information, any court orders or other legal restrictions, and the nature of the information being requested.

The centre will have regard to relevant Department for Education (DfE) guidance on parental responsibility, including guidance concerning:

- who has parental responsibility and the rights and responsibilities associated with it
- the rights of non-resident parents to receive information about their child's education

- circumstances in which information may be withheld where disclosure could result in serious physical or mental harm
- the role of a local authority acting as a 'corporate parent'; and
- the provision of GCSE results and other educational information to parents

The current DfE guidance is Parental responsibility: guide for schools and local authorities, including *Understanding and dealing with issues relating to parental responsibility*, which was last updated on 24 August 2023.

The centre will also have regard to the DfE guidance School reports on pupil performance: guide for headteachers, which sets out requirements concerning information that schools must provide to parents, including grades achieved in GCSEs and other qualifications. This guidance was last updated on 8 May 2024.

Parents and persons with parental responsibility

Where a parent or other person with parental responsibility requests examination-related information, the centre will establish, where necessary, the identity and status of the person making the request and consider whether the information should be provided under the relevant education legislation and guidance.

A non-resident parent who has parental responsibility will not automatically be excluded from receiving educational information simply because they do not live with the child. The centre will consider the individual's legal rights and any relevant court order or other restriction before deciding whether information can be disclosed. DfE guidance confirms that GCSE results form part of the pupil's educational record and may be disclosed to a parent on request; the pupil's consent is not normally required. However, information may be withheld where the school considers that disclosure could result in serious physical or mental harm to the pupil or another individual.

Where a parent or other person with parental responsibility requests information about a child who is 16 or over, the centre will consider the applicable education-law provisions, the young person's circumstances and any relevant restrictions before disclosing information. Data protection rights will also be considered where the requested information constitutes the young person's personal data.

Local authorities and corporate parents

Where a local authority or another person is acting in a corporate parenting capacity, the centre will consider whether the requesting organisation or individual has a lawful entitlement or other appropriate legal basis to receive the information.

The centre will not assume that a local authority is entitled to receive all information about a child simply because it has corporate parenting responsibilities. The nature of the request, the authority or individual's legal role, the information requested and any applicable legal requirements will be considered before information is disclosed. Relevant information-sharing arrangements and statutory duties will also be taken into account.

Data protection considerations

Where examination information constitutes personal data, any disclosure must also comply with applicable UK data protection legislation, including the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025.

The centre will ensure that personal data is disclosed only where there is an appropriate lawful basis and the disclosure is necessary and proportionate. The centre will take particular care where information includes special category data or other confidential or sensitive information.

Where there is uncertainty about whether information can be disclosed, the request will be referred to Ms Alford before information is released.

The centre will maintain an appropriate record of significant decisions concerning the disclosure or withholding of examination-related personal data, particularly where there is a dispute concerning parental responsibility, a court order, safeguarding concern or other legal restriction.

Publishing exam results

When considering whether and how to publish examination results, Loreto Grammar School will comply with applicable UK data protection legislation and have regard to relevant guidance issued by the Information Commissioner's Office (ICO), the Department for Education (DfE) and the Joint Council for Qualifications (JCQ).

The centre may publish examination results, including in the local or national media or on the centre's website or premises, where this is permitted by law and is consistent with the centre's stated purposes for processing personal data.

The centre will:

- act fairly and transparently when publishing examination results
- ensure that pupils and their parents or guardians are informed as early as reasonably practicable whether examination results will be made public and how they will be published
- explain the form in which results will be published, for example whether candidates will be listed alphabetically, by subject or qualification, or according to grades achieved
- publish only information that is appropriate and necessary for the stated purpose
- take reasonable steps to minimise unnecessary disclosure of personal information
- have regard to relevant JCQ requirements concerning the release and confidentiality of examination results; and
- take seriously any concerns or objections raised by a pupil or their parent or guardian about the publication of examination results

The centre does not normally require the consent of pupils, parents or carers to publish examination results where the publication is undertaken on an appropriate lawful basis. The UK GDPR does not prevent schools from publishing examination results in the local press or online.

However, pupils and parents or guardians should be given an opportunity to raise concerns or object to the publication of results. Where an objection is received, Mrs Stokes will consider the circumstances and determine whether the proposed publication should proceed. The centre will take the objection seriously and will not reject it without good reason.

Where appropriate, the centre will consider factors such as:

- the nature and purpose of the proposed publication
- the information that would be disclosed
- the potential impact on the pupil
- the pupil's age and circumstances
- whether the pupil or their parent or guardian has raised specific concerns

- whether publication is necessary and proportionate for the stated purpose; and
- whether the information can be published in a way that reduces any unnecessary impact on the individual

Where an objection is rejected, the centre will provide the individual with an explanation of its decision.

The centre will also ensure that examination results remain strictly confidential until the relevant awarding organisation's authorised release date. Results received by schools and colleges before results day must not be disclosed prematurely.

Further information about the publication of examination results and data protection is available from the Information Commissioner's Office.