MOUNT ST MARY'S CATHOLIC HIGH SCHOOL

Educating the Individual for the Benefit of All

DATA PROTECTION POLICY

Mount St Mary's Catholic High School Data Protection Policy

Adopted by Mount St Marys' Governing Body on 20 September 2022

Signed Chair of Governors

Review date: 20 September 2025

Mount St Mary's Catholic High School's (MSM) Aims

- To ensure that all personal data it collects and/or processes on individuals does so in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018
- To ensure that the data protection rights of students, staff and other members of the MSM community are safeguarded

The following policy details how MSM does this; it refers to all personal data regardless of the format in which it is stored or processed. It refers to policy regarding public examination data, but for more specific details, please refer to the specific exam related policies

Personal data protection principles

There are 6 data protection principles with which MSM must comply.

The principles state that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes – if these change at all, the data subjects would always be informed prior to the changes commencing
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Legal entitlement to collect and process personal data

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

As a school, MSM is categorised as a public authority and as such conducts its operations in "the public interest" and the vast majority of the data collection and processing at MSM is categorised by this legal entitlement. Where data collection and processing at MSM would not be categorised by "the public interest" category, consent from the individual subjects would need to be sought first, or from those with parental responsibility for the subject. Once consent has been given it can be withdrawn at any point, so long as it is for a valid reason. Consent will always be sought from those with parental responsibility for all children under the age of 13 and consent can be withdrawn at any point thereafter. Once the subject reaches the age of 13 they have the right to withdraw consent or give it themselves unless MSM feels strongly that the subject does not have the maturity to make such a decision, in which case those with parental responsibility will be approached for consent. MSM takes the stance that once parental consent, or that of a newly arrived student of 13 years of age or more, has been given it will be for the duration of the student's time at MSM unless consent is withdrawn by the student until the student is in Year 9 and then from September we will seek consent renewal directly from the student annually.

Collecting personal data

There are 3 main ways in which MSM obtains information about students and parents:

1. Passed on to MSM from a student's previous school in Great Britain, from a Local Authority (LA) or the Department for Education (DfE)
2. Parents, guardians or carers complete information request forms if there is no previous school in Great Britain
3. Gathered as student progresses through MSM

There may be rare occasions when information is passed to MSM by other third parties, but in such situations, reasonable efforts are always made to check the accuracy of the information.

What personal data MSM collects

Student

- Personal information (such as name and address and those of each student's parents, guardians, carers and other contacts)
- Characteristics (such as medical and health information, ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Details of care and support provided
- Academic performance and public exam related data
- Behaviour records
- Photographs, video and audio recordings – photographs used on the students' files are for identification only and as such require no consent. Use of photographs, video and audio recordings for other purposes will only occur when consent has been sought and granted unless it is for exam related assessments.
- CCTV images captured – CCTV is used in accordance with the ICO code of practice for the use of CCTV for the purposes of crime prevention and the safety of the individuals of the MSM community and any visitors to the MSM site. No additional software such as face recognition is used.
- Biometric recognition systems fingerprints using fingerprint digital imaging is used for cashless catering and printing. This is done in compliance with the Protection of Freedom Act 2012.
    - Consent for inclusion in these systems will be sought prior to inclusion and consent can be withdrawn at any time
    - If consent is withheld or withdrawn then alternative methods will be found for both catering payment and printing and any such data held will be immediately deleted

Staff

- Contact details
- Some personal and sensitive data
- Banking details
- Vehicle details
- Next of kin for emergency contact
- Details of training
- Details of employment
- Photographs, video and audio recordings – photographs used on the staff files are for identification only and as such require no consent. Use of photographs, video and audio recordings for other purposes will only occur when consent has been sought and granted.

- CCTV images captured – CCTV is used in accordance with the ICO code of practice for the use of CCTV for the purposes of crime prevention and the safety of the individuals of the MSM community and any visitors to the MSM site. No software additional software such as face recognition is used.
- Biometric recognition systems fingerprints using fingerprint digital imaging is used for cashless catering and printing. This is done in compliance with the Protection of Freedom Act 2012.
    - Consent for inclusion in these systems will be sought prior to inclusion and consent can be withdrawn at any time
    - If consent is withheld or withdrawn then alternative methods will be found for both catering payment and printing and any such data held will be immediately deleted

Parent/carer

- Contact details and details of the relationship to the student
- CCTV images captured – CCTV is used in accordance with the ICO code of practice for the use of CCTV for the purposes of crime prevention and the safety of the individuals of the MSM community and any visitors to the MSM site. No additional software such as face recognition is used.

Service providers/contactors

- Contact details
- Agency or firm for/with whom they work
- Role within the agency or firm
- CCTV images captured – CCTV is used in accordance with the ICO code of practice for the use of CCTV for the purposes of crime prevention and the safety of the individuals of the MSM community and any visitors to the MSM site. No software additional software such as face recognition is used.

Why MSM collects personal data

- To support student learning
- To monitor and report on student progress
- To provide appropriate pastoral care
- To assess the quality of our services
- Protect student welfare
- Administer admissions waiting lists
- Carry out research for the development of educational practice
- Comply with the law regarding data sharing

All the information that MSM collects is essential to performing its normal day-to-day tasks as a school to the best of MSM's ability. The student and parent/carer data enables good home school communication, helps to support student health and education, and provides information that could be important for health and safety reasons; it also enables MSM, our LA Leeds City Council (LCC) and the DfE to monitor and analyse student performance to aid in development of educational provision for future students of similar educational need and ability.

Because MSM has a legal basis for its operations, the provision of the information outlined above to MSM by those responsible for the students that attend MSM is mandatory. Where data provision is voluntary, MSM is legally required to seek consent to either gather or process such a data type and it will always undertake to do so.

Personal data storage and security

- Personal data is largely stored electronically at MSM, but some hard copy data is also stored in locked filing cabinets. Some personal data is stored in both electronic and hard copy formats. This includes all exam related data
- All hard copy personal data is stored in locked filing cabinets and the persons with responsibility for collecting and processing the personal data contained therein have the keys
- Access to the MSM Management Information System (MIS) where the electronic personal data is stored is controlled by levels of permission and password protection
- MSM staff are obliged to lock computer workstations upon leaving said workstation, or the room in which they are working upon exit so long as the workstation screen is not visible from outside the room
- MSM staff are encouraged to refrain from using mobile memory devices to store any personal data but if they do they are requested to use encrypted mobile devices; from Easter 2019 they will be obliged to an MSM controlled and managed encryption software called "Bit Locker" produced by Microsoft.
- MSM's computer network is protected by firewalls, the internet provider's security measures and internal anti-virus software
- Access to the MSM network is password protected and therefore limited to those with access permission
- Any electronic copies of personal data not stored on the MSM MIS is stored on the MSM network
- The taking of personal data in any form off the MSM site is strictly restricted (see MSM ICT Policy for further details)

Personal data retention and disposal

- MSM only retains any personal information gathered by MSM for as long as necessary to satisfy the purpose for which MSM collects it.
    - Recommended periods for data retention vary with no national definitive, but the accepted retention period for any student personal data is up to the student's 25th birthday. Extenuating factors can extend the retention period. (See Appendix 2 for MSM information retention periods which have been based upon those recommended by the Information and Record Management Society (IRMS))
- Personal data will only be kept for as long as it might be needed
    - This will include archiving the data for future comparative use in aid of statistical analysis and possible research
- The management information system automatically deletes sensitive student information once a student leaves MSM
- All records containing personal data are made either unreadable or un-reconstructable by:
    - Shredding paper records which are then removed by a waste paper merchant
    - Personal paper records are collected and destroyed by a commercial paper shredding company
    - Cutting CDs and DVDs into small pieces
    - Any audio or video tapes are dismantled and shredded
    - Hard disks are dismantled and physically damaged e.g. with a hammer or sanded
- For more detail on secure destruction of electronic storage devices please see the MSM ICT Policy

Sharing personal data and data disclosures

MSM is obliged to share personal data with the DfE, LCC and schools to which students may transfer, beyond this, MSM will not normally share personal data with anyone else including the media, but may do so where:

- There is an issue with a student or parent/guardian/carer that puts the safety of MSM staff at risk
- Where written consent has been given by the parent/guardian/carer; or by the student if they require their public exam results to be collected by someone other than themselves
- Liaison with other agencies is required – MSM would seek consent as necessary prior to doing this
- Exam entry data and non-exam assessment data, is sent to the relevant examination boards electronically. The exception to this is Art & Design work which is held on site and internally moderated by an external moderator

- Examination Access Arrangement data is currently held in hard copy in locked cupboards in the exams' storage room and the SEND office
- MSM's suppliers or contractors need data to enable MSM to provide services to our staff and students – for example, IT companies. When doing this, MSM will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with current data protection law
    - Where necessary, 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
    - Where necessary, only share data that the supplier or contractor needs to carry out their agreed service, and information necessary to keep them safe while working with us. Assurances would be obtained that any data held would be deleted upon termination of the account

MSM will also share personal data with law enforcement and government bodies where it is 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

MSM may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any MSM students or staff.

Whilst MSM does not anticipate transferring personal data to a country or territory outside the European Economic Area, if it were necessary it would be done in accordance with current data protection law.

Roles and responsibilities

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

MSM collects and processes personal data relating to parents, students, staff, governors, visitors and possibly other individuals, and therefore is designated a data controller. MSM is registered as a data controller with the Information Commissioner's Office (ICO) and renews this registration annually.

MSM Governing Body

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

The Headteacher

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

The Examinations Officer (EO)

The EO is responsible for implementing, managing and overseeing all aspects of Public Examinations conducted at MSM

Data protection officer

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

The DPO 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 MSM data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes. Any communication for the DPO should be addressed to:

MSM DPO
Ellerby Road
Leeds
West Yorkshire
LS9 8LA
Email: DPO@mountstmarys.org

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the MSM DPO in the first instance.

To make a complaint, please contact MSM DPO as above.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

All MSM staff

Are responsible for:

- Collecting, storing and processing various personal data in accordance with this policy
- Informing MSM of any changes to their own personal data, such as a change of address
- Familiarising themselves with and adhering to the MSM Data Protection Policy
- Contacting the MSM DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging, about to engage or planning to engage in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties should the need arise, and if it did, consent from the data subjects would always be sought first

MSM Students and their parents, guardians or carers

All have a duty to ensure that all personal data supplied to MSM is accurate and up to date at all times

Rights of MSM Students and their parents, guardians or carers

Requests for information can be made:

- Under the Freedom of Information Act (2000) (FOIA)
    - Can be made by anyone but personal data should not be given in response to an FOIA request
- Via a "Subject Access Request" (SAR) (Requesting to see the personal information held by MSM)
    - Can only be made by the data subject (whom the data is about), the data subject's parents/guardians/carers if the subject is under 13 or adjudged unable to make the SAR themselves, or someone else that has proven permission from the subject

Making a SAR

Any individual, of 12 years of age or more, on which MSM holds personal data has a legal right to request access to the information, any such requests should be directed in writing, either by letter, email of fax to: The Data Protection Officer for MSM.

Acceptance of verbal SARs would depend on the situation and be considered on an individual basis, but normally verbal SARs would not be encouraged without written confirmation.

When making a SAR, MSM would prefer that the SAR form in Appendix 2 be used as this will make processing the SAR much easier.

The same individuals 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 (not a system currently employed by MSM)
- 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

Parents, guardians or carers can make a request with regard to their child's data where the child is under 12 without the child's consent as such children are regarded as having insufficient maturity to make the SAR themselves. Regardless of age, the data about the student belongs to the student and no one else, but if under 12 years old their parents, guardians or carers have the same rights as their child as their representative. Parents, guardians and carers also have a right to request the information about themselves that MSM has collected, stored and processed.

It should be stressed, that MSM only gathers and processes information that it is legally bound and legally able to do so. Consent for storage and processing of any information that does not fall within the legal necessity to operate as a school is always sort e.g. the use photographic material in newspapers.

MSM response to a SAR

In the interest of data security, MSM will only reply to a SAR if there is proof of identity of the person making the SAR. Proof is ideally a photographic ID such as driving license or passport, however, if MSM staff can vouch for the identity of the person making the SAR and their relation to the person about whom the SAR has been made, the SAR can be accepted. If a SAR is made about a subject of 12 or more years of age, consent for the SAR would also be sought from the subject. Although, this is not always the case as the maturity of a subject of 12 years or more of age might be adjudged insufficient to make the SAR such judgement will always be made on a case-by-case basis.

In the event of a SAR, if MSM does hold information on the "subject", the following information can be expected in the MSM response:

- Confirmation that the subject's personal data is held and being processed
- A description of what is held
- An explanation of why it is held and being processed, and how long it will be retained
- An explanation of where and how the data was obtained if not from the "subject"
- With whom it has been shared or will be shared with
- Let you know if any "automated decision making" has been applied to the data and any consequences of this – does not currently happen at MSM

MSM's reply to the SAR could be sent electronically or in hard copy depending on the SAR. Any response to a SAR will always be free of charge and would occur within 1 calendar month from the date of the day following receipt of the SAR. However, in the case of complex or numerous SARs, MSM would inform the requestor of the need to extend the response period to 3 months and explain why this is necessary.

MSM reserves the right not disclose information if it:

- Might cause serious harm to the physical or mental health of the subject or another individual
- Would reveal that the subject is at risk of abuse, where the disclosure of that information would not be in the subject's best interests
- Is contained in adoption or parental order records

- Is given to a court in proceedings concerning the subject

If the SAR is unfounded or excessive, MSM may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A SAR will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

On occasions where MSM refuses to reply to a SAR, the requestor would be told why and tell them they have the right to complain to the ICO.

Other rights

Under data protection law, individuals have certain rights, outlined below, regarding how their personal data is used and kept secure including the right to:

- Withdraw consent to data processing, where it was required, at any time
- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Be notified in the event of a data breach that might directly affect them
- Claim compensation for damages caused by a breach of the data protection regulations
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

To exercise any of these rights, please contact the MSM DPO.

MSM DPO
Ellerby Road
Leeds
W.Yorkshire
LS9 8LA
Email: DPO@mountstmarys.org

Any staff that receive a SAR should pass it directly on to the MSM DPO.

Data breaches at MSM

Any data breach, accidental or otherwise, will be dealt with in the following manner

1. Report the breach or suspected breach to the DPO as soon as identified or suspected
2. The DPO, with the MSM ICT Team will then investigate the notification, contain any issues found and minimise the impact that may be had
3. If the breach is verified, it will first be assessed for severity and the potential impact upon any or all individuals on whom personal data is stored and processed by MSM
4. If the breach is severe and/or there is a high risk of adversely affecting individuals' rights or freedoms, those affected will be informed immediately and The Information Commissioner's Office (ICO) will be informed within 72 hours of becoming aware of the breach and required information will be given to ICO freely
5. Any additional relevant third parties that may be able to assist in mitigating any loss or discovering the origin and cause of the breach will also be notified e.g. police, insurers
6. The investigation into the breach will be reviewed and measures will be put in place to remedy the breach and prevent further occurrences of similar breaches so far as possible
7. Everything done at each step will be recorded as will every breach or suspected breach regardless of the severity. This will serve as an audit trail in the event of complaint or challenge from ICO and as e reference tool for possible future issues

Complaints

MSM takes any complaints about its collection and use of personal information very seriously.

If you think that MSM's collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about its data processing, please raise this with MSM in the first instance using the complaints form in Appendix 3 and sending it to the MSM Data Protection Officer.

Alternatively, if you are unhappy with MSM's response to your complaint, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If you would like to discuss anything in this privacy notice, please contact:

The MSM Data Protection Officer.
MSM DPO
Ellerby Road
Leeds
W.Yorkshire
LS9 8LA
Email: DPO@mountstmarys.org

Appendix 1

Glossary of terms

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Automated decision-making	A decision made without any human involvement, triggered by specific data.

Appendix 2

Data Retention Schedule

Data Type	Retention period	Outline of data retained
Student	Student's 25th birthday	Basic. Nothing sensitive
Employee	6 years after leaving MSM	Basic. Nothing sensitive or financial
Parent	Student's 25th birthday	Basic. Nothing sensitive
Governor	Nil. Immediate deletion upon leaving	N/A
Volunteer	6 years after termination of association in case required again	Basic
Job Applicant	6 months in case of call back	All details contained in the application
Agency worker	6 years. In line with financial records retention	Basic
Contractor	6 years. In line with financial records retention	Basic
Supplier	6 years. In line with financial records retention	Basic

Appendix 3 – Table recording candidate exams-related information held

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Access arrangements information	Hard copies in files	Candidate name Candidate DOB Gender Data protection notice (candidate signature) Diagnostic testing outcome(s) Specialist report(s) (may also include candidate address) Evidence of normal way of working	Examination Admin room In secure office (SENDCo)	Lockable metal filing cabinet in the	3 years Sent to student's next educational establishment at the request of either
Alternative site arrangements	n/a				
Attendance registers copies		Candidate name Exam number	File in Exams Office	Locked cupboard	
Candidates' scripts		Name and exam number	Exams Storage Room	Secure cupboard	
Candidates' work		Name and exam number	Department Office	Secure Store	
Centre consortium arrangements for centre assessed work	n/a				
Certificates		Name and qualification	Certificate Cupboard in the Exams Office	Locked cupboard	

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Certificate destruction information		Name and qualification	Certificate Cupboard in the Exams Office	Locked cupboard	
Certificate issue information		Name and qualification	Certificate Cupboard in the Exams Office	Locked cupboard	
Conflicts of interest records		Nam and details	Exams Officer's drive on the MSM network	MSM network is password protected	
Entry information		Name and exam number DOB	SIMS	Password protected	
Exam room incident logs		Name, exam number, details and evidence	Exams Office	Locked cupboard	
Invigilator and facilitator training records		Name of invigilator	Exams Office	Locked cupboard	
Overnight supervision information		Name, exam number and details	Exams Officer's drive on the MSM network	Password protected	
Post-results services: confirmation of candidate consent information		Name, exam number and details	Exams Officer's drive on the MSM network	Password protected	
Post-results services: requests/outcome information		Name, exam number and details	Exams Officer's drive on the MSM network	Password protected	

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Post-results services: scripts provided by ATS service		Name, exam number and details	Exams Officer's drive on the MSM network	Password protected	
Post-results services: tracking logs		Name, exam number and details	Exams Officer's drive on the MSM network	Password protected	
Private candidate information		Name, exam number and DOB	Exams Officer's drive on the MSM network	Password protected	
Resolving timetable clashes information		Name, exam number and details	SIMS	Password protected	
Results information		Name and qualification grades	SIMS SISRA Exams Office	Password protected Password protected Locked cupboard	
Seating plans		Name and exam number	Exams Office	Locked cupboard	
Special consideration information		Name, exam number, details and evidence of special consideration	Exams Office	Locked cupboard	
Suspected malpractice reports/outcomes		Name, exam number, details and evidence	Exams Office	Locked cupboard	
Transferred candidate arrangements		Name, exam number	Exams Office	Locked cupboard	

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Very late arrival reports/outcomes		Name, exam number and details	Exams Office	Locked cupboard	