Manchester Hospital School

Data Protection Policy

Document Control	
Title	Data Protection Policy
Policy Number	MHS023
Date	September 2026
Supersedes	September 2025
Purpose of the policy	Set out processes, procedures, and responsibilities for handling personal data in compliance with UK data protection legislation across all school functions.
Related policies/guidance	Data Protection Act 2018; Data (Use and Access) Act 2025; DfE Data protection: toolkit for schools; Information Commissioner's Office (ICO) / Information Commission guidance; The Exams Office - Data Protection Policy (Exams).
Review	September 2027
Author	Danielle Clough
Date Consultation Completed	September 2026
Date adopted	**13th October 2026 at Full Governing Body meeting**

Under the Public Sector Equality Duty, Manchester Hospital School has due regard to the need to eliminate discrimination, harassment and victimisation and any other conduct prohibited by the Equality Act 2010; to advance equality of opportunity between those who share a relevant protected characteristic and those who do not share it and to foster good relations across all protected characteristics. Manchester Hospital School will take into account equality considerations when policies are being developed, adopted and implemented.

Manchester Hospital School serves the needs of a very large and diverse range of children, young people and their families at times when they are extremely vulnerable. Our core purpose as a school is to uphold the child's right to Education and our policies and procedures are necessary to keep staff and children safe . We acknowledge that our students are often living with a range of very complex medical conditions including mental ill health and therefore we keep the needs of the student at the heart of all decisions. We will , therefore, work within the parameters of all statutory policies whilst seeking to understand and support the child's long term education and health needs.

Introduction
The school must process personal data to fulfil its obligations as an employer and education provider. The school is committed to ensuring that the personal data we process is done so in accordance with the high standards set by data protection law in the United Kingdom (UK). This policy outlines how we comply data protection law.

A key of useful data protection terms has been included at appendix 1.

Legal Framework
When processing personal data, the school complies with the following primary legislation:

- UK General Data Protection Regulation (UK-GDPR)
- Data Protection Act (DPA) 2018
- Data (Use and Access) Act 2025

In addition to the key legislation defined above, the school follows guidance and standards set by the following bodies:

- Information Commissioner's Office (ICO) / Information Commission
- Department for Education (DfE)
- Information Records Management Toolkit for Schools (IRMS)

This policy is linked to the following documentation:

- Records Management Policy & Retention Schedule
- CCTV Policy
- Safeguarding Policy

Scope
This policy applies to all personal data processed by the school along with any information processed by third-party Data Processors and Joint Data Controllers. For the purposes of this policy, personal data is any information relating to an identifiable individual that is held on a physical or electronic filing system.

This policy applies to those individuals whose personal data is processed by the school namely:

- Pupils (including prospective pupils)
- Parents & Guardians
- Staff (including applicants)
- Governors & Volunteers
- Contractors
- Visitors

Data Controller
The school is the 'Data Controller' for the personal data that we process which means that we are responsible for that data and make key decisions on how it is used. The school is registered with the ICO and renews its subscription annually.

Data Protection Officer (DPO)
The school has appointed a Data Protection Officer (DPO) to oversee compliance with this policy and the aforementioned data protection legislation. Our DPO is Miss Danielle Eadie of RADCaT Ltd who is supported internally by the school's leadership team.

Our DPO acts as the first point of contact for the ICO and those individuals whose personal data is processed. Our DPO can be contacted directly using the following details if there are any questions about this policy or data protection in general:

DPO: Miss Danielle Eadie

A: RADCaT Ltd, 6 Seven Stars Road, Wigan, WN3 5AT

T: 01942 590 785 | e: Danielle.eadie@radcat.co.uk

Responsibilities
This policy applies to all staff employed by the school and those working with us on a temporary and / or voluntary basis. Third-party individuals or organisations contracted to process personal data on our behalf will be required to comply with this policy.

The Board of Governors

The Board of Governors has an overall responsibility for ensuring that the school complies with its data protection obligations.

Headteacher and Senior Leadership Team (SLT)

The school's senior leadership team are responsible for allocating the resources required to meet and maintain high standards of data protection compliance. The senior leadership team will oversee and communicate the provisions of this policy. In conjunction with the DPO and governing board where necessary, the senior leadership team will be responsible for making decisions regarding data processing.

All Staff

All staff (including temporary staff, volunteers and contractors) are responsible for processing personal data in accordance with this policy. Staff members that do not adhere to this policy may face disciplinary action.

The school ask that all staff contact the DPO without undue delay if the following situations:

- They have questions or concerns regarding this policy, data protection law, retaining personal data or how to keep information secure and confidential.
- There are concerns that this policy is not being followed.

- They wish to engage in a new activity that involves processing personal data.
- They are asked to share personal data with a third party.
- A data breach, near miss or gap in security has been identified.
- They receive a request regarding the rights of individuals such as requests for copies of personal data.

The school ask that all staff inform us in a timely manner if there are any changes to their own personal data such as address and contact details.

Data Protection Principles
The UK-GDPR sets out six key principles that the school must comply with to ensure personal data is secure and confidential. The UK-GDPR asks that personal data is:

Processed lawfully, fairly and in a transparent manner

Lawfulness:

The school will not process personal data unless it can meet **one** of the lawful bases (legal reasons) set out in Article 6 of the UK-GDPR:

- The school must process personal data to comply with a **legal obligation**.
- The school is required to process personal data to fulfil a **contractual obligation** with the individual.
- Personal data must be processed for the performance of a task in the **public interest**; the school must process personal data to meet its official functions as an education provider.
- Personal data needs to be processed in the act of protecting or saving someone's life; the school has a **vital interest** to process personal data in such situations.
- Personal 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 / guardian in respect of younger pupils) has provided their **consent** to process their personal data.

When processing special categories of personal data, the school will meet an additional lawful basis from Article 9 of the UK-GDPR and Data Protection Act which are summarised here: What are the conditions for processing? | ICO

Conditions that the school will typically rely upon include:

- Special category data is being processed in the field of **employment, social security and social protection.**
- The school has deemed there is a **substantial public interest** to process the special category data.
- The individual has provided their **explicit consent** (written) permitting the school to process their special category data.

Fairness and Transparency:

Prior to the processing of any personal data taking place, the school will inform individuals what data will be collected, how it will be used and why; individuals are also informed if data processing is mandatory or optional and their consent is required.

Consent

Where consent is the lawful basis relied upon for the processing of personal data, the school will ensure that the individual (or their parent / guardian in respect of younger children):

- Have a clear understanding of what they are consenting to and why.
- Understand that they have a choice and can change their mind at any time.
- Are provided with instructions on how to withdraw their consent should their preferences change.

The school issue consent forms as part of the pupil admissions pack for routine activities that require consent; a log of consenting pupils is kept and reviewed on an annual basis. Consent based activities for staff are much less frequent with permission sought on an ad-hoc basis.

Consent can be withdrawn at any time by contacting the school office.

Consent and Pupils

Pupil personal data belongs to the pupil and not their parent or guardian. However, the school understands that some pupils (dependent upon age) may not be mature enough to understand their rights regarding data protection, consent will therefore be sought from the parent or guardian.

It is typically accepted that pupils in primary school are too young to understand and make decisions about their own data. Any consent required will therefore be sought from the parent or guardian.

Purpose Limitation

The school will not process personal data unless there is a valid purpose for doing so, nor will we use data for a new purpose without informing individuals and seeking their consent where applicable. The school will explain the reasons for processing to individuals at the point of collating their personal information.

Staff within the school should not process personal data for any new purposes outside of their approved duties without permission; the SLT and / or the DPO should be consulted beforehand.

Data Minimisation

The school will only process the minimum amount of data necessary to fulfil the purposes for which it was collected. Data collection forms and platforms are carefully designed to ensure only categories of data that are strictly necessary will be inputted to ensure staff and individuals do not provide any excess data. The school adopts a minimalist approach to data sharing and prompts staff to always question what is absolutely necessary.

Special categories of personal data should only be shared or processed if it is absolutely necessary; staff should seek approval if there are any concerns or doubts.

Data Accuracy

The school makes reasonable attempts to ensure personal data is up to date and accurate. Checks are performed at least annually to ensure basic pupil and staff data such as contact details are accurate. Similarly, consent is reviewed and updated on a routine basis to avoid processing data without a lawful basis.

The school has implemented information management systems that integrate with other key software meaning that changes to data are automatically updated across the board.

Meeting notes and key records are reviewed by relevant parties prior to finalising to ensure a uniform agreement to the content. Staff are encouraged to keep records factual and succinct.

If reasonable attempts to rectify incorrect information are not possible, the school will ensure records are securely deleted.

Storage Limitation

Personal data will only be kept for as long as necessary to fulfil the purposes for which it was collected; records will not be kept 'just in case' they may be needed in future.

The school has implemented a 'Records Management Policy and Retention Schedule' that provides guidance on how long personal data should be kept and the approach taken by the school to manage those records in line with data protection legislation.

The school performs a review of records at least annually to ensure that any records no longer required are securely disposed of. Automated deletion should be applied where necessary for any electronic records that do not require a manual review.

Please refer to our 'Records Management Policy' for more information.

Integrity and Confidentiality (Data Security)

The school must ensure that adequate control measures are in place to protect the integrity and confidentiality of the personal data that we process in both physical and electronic formats. Security is a vital element in the school's approach to data protection and high standards are achieved by the following key control methods:

- Ensuring a clear desk at all times; documents and data storing devices such as laptops, mobile phones and tablets should not be left unattended; routine walkaround checks are made to assess compliance.
- Physical records and devices to be kept in locked cabinets with key access strictly limited.
- Auto lock activated on all devices and screens locked if a staff member leaves their workspace.
- A full and up to date asset and software register to map out where data is stored that includes a log of devices / records that are taken off site.
- Access controls in place on all records to ensure staff only access the records they need to perform their roles.
- User accounts and devices issued to individual staff members will not be shared with other users.

- Passwords changed on a routine basis and must contain a combination of letters, numbers and special characters; multi-factor authentication will be utilised where available.
- A process to ensure all visitors to site are effectively managed and not permitted entry without an ID badge and DBS checks where necessary.
- Staff receive routine training on data protection and security, sign confidentiality and acceptable use agreements and partake in DBS checks.
- Access to records and user accounts is to be removed without undue delay if a staff member leaves their employment; an exit checklist is in place.
- Compliance checks and 'Data Protection Impact Assessments' (DPIA) where necessary performed on data processing suppliers.

The school monitors compliance checks with the above control measures by performing regular audits on security which includes:

- Routine walkaround checks on a departmental level to identify any areas of non-compliance.
- Annual audit performed by the DPO to assess the school's compliance with the principles of the UK-GDPR; a report will be provided.
- Regular gap analysis and monitoring on school systems performed by the ICT department(s) to highlight any gaps in security.
- External audits performed at intervals.
- **Prohibition of Unauthorised Recording Devices:** The use of personal wearable recording hardware (including smart glasses) is restricted on school grounds to prevent unauthorised data capture or privacy breaches.

Accountability
Accountability is the overarching principle of the UK-GDPR and requires the school to demonstrate how it complies with the six core principles. The school achieve accountability by:

- Implementing key data protection policies and procedures and communicating these with staff and other relevant parties.
- Applying the core data protection principles in other key operational areas of the school namely; HR, Marketing, Finance, Health & Safety and Safeguarding.
- Keeping adequate logs of data breaches and reviewing logs on an annual basis to assess areas for improvement.
- Keeping records of consent, requests regarding the rights of individuals and decision making.
- Keeping a 'record of processing activities' that clearly outlines an up-to-date inventory of data, the purposes and lawful bases for processing and key characteristics regarding how that data is managed.
- Implementing data sharing agreements and compliance checks on third party Data Processors and Joint Controllers.
- Completing 'Data Protection Impact Assessments' where necessary on any high-risk data processing areas.

Data Sharing
The school must share personal data to meet its legal and operational obligations as an employer and education provider. Routine data sharing is limited to the following:

- Statutory data collections submitted to the Local Authority and Department for Education.
- Transfers of records between educational settings.
- Transfers of data to and from the government to meet a legal obligation (HMRC, Funding & Free School Meals etc)
- Liaising with or making referrals to third party agencies when additional support for staff or a pupil is required.
- Sharing data with our suppliers and providers of professional services if it is required to fulfil their services to us (IT, Payroll, Legal Advisors etc)

In certain circumstances, the school must share personal data with law enforcement, governing bodies and legal entities when required to do so to including:

- In the prevention and detection of crime and to apprehend offenders.
- In connection with legal proceedings and claims.
- A significant safeguarding concern has been identified.
- Supporting the emergency services if an accident or incident has occurred.
- Supporting an investigation.

When sharing information with third parties, the school will:

- Implement data sharing agreements that clearly outline the expectations and responsibilities of each party.
- Only share information with third party providers of services if they can guarantee that they comply with data protection law and high standards of security.
- Limit the personal data shared to what is absolutely necessary to fulfil the purpose of the data transfer.
- Keep a log of compliance documentation including data sharing agreements, privacy notices and security questionnaires.
- Complete DPIA's on any data transfers that pose a high risk the rights and freedoms of individuals.

The school asks that staff do not share personal data unless the transfer has been approved by their senior management with support from the DPO where necessary.

In respect of any personal data that is transferred outside of the United Kingdom, the school will ensure appropriate safeguards are in place that comply with data protection legislation. The DPO should be consulted for all transfers of data internationally. Staff should be aware that UK based companies may store personal data on international servers.

The Rights of Individuals

The UK-GDPR sets out 8 rights for Data Subjects that the school must comply with in certain circumstances:

- The right to be informed about how their personal data is processed.
- The right of access to their own personal data
- The right to rectification if they feel their personal data is incorrect or incomplete.
- The right to erasure (right to be forgotten)
- The right to restrict processing if they are unhappy with how their data is processed.
- The right to data portability
- The right to object to processing.
- Rights in relation to automated decision making and profiling.

The Right to be Informed

The school will issue 'Privacy Notices' to all parties whose data we process. Privacy Notices are issued at the start of our relationship with individuals to inform them what data we will collect, how it used and why we need it. We ensure that Privacy Notices are displayed in accessible locations for each party should they need to access them:

Data Subjects	Privacy Notice Issued:	Location
Pupils, parents & carers	In admissions pack	Website
Applicants	With application form (a link directing applicants to the relevant website section may be preferable)	Website
Staff	In induction pack	Staff Handbook or Shared Staff Policy Area.
Governors & volunteers	In induction pack	Shared Gov / Volunteer Policy Area.
Visitors	Notice in reception about where privacy information can be found.	Website and printable copies available at reception.

All school privacy notices will include the following:

- The name and contact details of the school as Data Controller
- The name and contact details of the DPO
- The categories of personal data being processed.
- How the information was obtained and whether processing is optional or compulsory
- The purposes for processing the data.
- The lawful bases for processing (including special categories of personal data)
- The recipients of personal data if shared with third parties.

- Details if personal data is shared outside of the United Kingdom
- Retention periods for the personal data
- The rights available to the individual
- The right to withdraw consent where applicable.
- The right to complain to the school and ICO (include instructions)

Privacy Notices are reviewed on an annual basis or sooner should a change in legislation or data processing activities occur.

The Right of Access

Individuals have a right to request access to the personal data that the school holds about them; this is referred to as a 'Subject Access Request' (SAR).

The school asks that requests be made in writing and include the individual's name, contact details, and specific details regarding the records they are looking to access. Requests should be sent directly to the DPO or to the school office, who will liaise with the DPO without undue delay.

In line with the Data (Use and Access) Act 2025, the school will conduct reasonable and proportionate searches to locate and retrieve the requested personal data. The school is not required to carry out searches that are disproportionate or excessively burdensome.

The school will assess the request to establish whether any of the following are required prior to processing:

- Proof of identity if there is any doubt the requester is who they say they are.
- Proof of parental responsibility if the request relates to a child and there is uncertainty that the individual has a legal right to act on behalf of that child.
- Consent from the pupil to share their records with their parent or carer if the pupil has been deemed mature enough to understand their data protection rights.
- A letter of authority if the request is made by a solicitor or representative on behalf of a client.

The school will confirm receipt of the request in writing, informing the individual that a response will be provided within one calendar month from the date the request was verified. If additional verification details are required, the response timeframe will commence once the school is satisfied the request is verified.

A response will inform the requester that:

- The request has been met in full and the relevant information enclosed.
- The school has deemed the request complex or voluminous and will exercise the right to extend the response time by a further two calendar months (three calendar months in total).
- The request has been refused (in full or part), including the specific legal exemption relied upon.

All responses will be accompanied by written details of the information provided, exemptions applied, a reference to the relevant Privacy Notice, and instructions on how to lodge an internal complaint or report concerns to the regulator.

Exemptions

A number of exemptions are provided in the Data Protection Act to cover scenarios when it may be inappropriate to disclose personal data as part of an information request. For example, if disclosure could cause serious harm to the individual or a third party.

The school will consult the DPO prior to providing any information if there are any concerns at all that disclosing the requested data could cause harm to the individual or another party.

Redactions

The school can only provide the individual with information about themselves and not that of any third parties without their consent unless we deem it reasonable to do so. Redactions to third party data will be applied where necessary.

In the case of pupil records, it is generally accepted that the identities of school staff, social workers and health professionals remain visible. Records will be reviewed on a case-by-case basis.

In situations where it is impossible to separate the individual's data from that of another person, the information may be omitted. The DPO will be consulted if there are any concerns regarding redactions.

A log of all information requests will be kept on the school's 'information request register'.

Right to Rectification

Reasonable attempts will be made by the school to ensure personal data is kept up to date and accurate. A check (at least annually) will be made to ensure basic identifiers and contact information is up to date; this will include details of emergency contacts.

Regular correspondence is made, and logs kept regarding allergies, medication and any special educational needs or health requirements to provide parents and guardians with the opportunity to request any changes.

Any data processing activities relying upon consent will be reviewed on an annual basis; consent will not be assumed.

Requests made to update basic information such as name changes and contact details will typically be fulfilled straight away by school staff. In situations where an individual makes a request to have more complex data rectified such as meeting notes, health and safeguarding records a review will be required with input from the SLT and DPO.

Right to Erasure

The right to erasure will only apply in certain circumstances as the school has legal and operational obligations to retain data. The right to erasure will apply in the following circumstances:

- consent is the lawful basis for processing; the individual has a choice.
- the data is no longer necessary for the purpose in which it was collected.
- the processing is determined to be unlawful.
- there is a legal obligation to remove the data.

In such circumstances, the school will securely dispose of the personal data in question and a confirmation will be provided to the individual.

In the event that a request to be forgotten cannot be met, the individual will be provided with an explanation which includes the set retention period for their personal information.

Right to Restrict Processing

The right to restrict processing is not an absolute right and will only apply in the following situations:

- The individual contests the accuracy of their personal data.
- The individual challenges the school's lawful basis for processing their data.
- The school no longer needs the data but the individual asks that we retain their records for the establishment, exercise or defence of a legal claim. The school will continue to store the data but will not process it any further.
- The lawful basis is legitimate interests, and the individual feels their own interests are being overridden by the processing.

The school will refrain from processing for a temporary period whilst a review into the individual's request is reviewed.

Individuals will be provided with an outcome of their request that includes details on whether or not processing will continue along with the reasons why.

Right to Object to Processing

There are three main instances in which individuals have a right to object to the processing of their personal data:

- The processing of personal data is for the purposes of direct marketing; the processing is therefore optional.
- Personal data is being processed for scientific, historic or statistical research purposes unless the processing is necessary for the performance of a task in the public interest.
- The lawful basis for processing is for the performance of a task in the interest of the public or legitimate interests.

Where the processing of personal data is optional, the school will remove the individual's data if an objection request is received.

The school does not process personal data for research purposes unless it is strictly necessary for the performance of a task in the public interest. We will however review such requests and provide an explanation to the individual if their request cannot be met.

Should the lawful basis for the data in question be a public task or legitimate interests, the school must demonstrate compelling grounds to continue processing following receipt of an objection request. The school must justify why the processing overrides the individuals' own interests.

Data Portability

The school understands that individuals have a right to ask that any data they provide to us is transferred from one IT environment to another by automated means between Data Controllers. It is not anticipated that there are any instances in which this right would currently apply to the school processing of personal data, we will however review any requests with the DPO.

Automated Decision Making & Profiling

The school does not currently partake in any data processing based upon automated decision making and profiling. Whilst some systems incorporate features associated with automated decision making, AI for instance, the school will always ensure that such elements are not used solely without any human involvement.

Human intervention **must** always be applied to any systems or processes that involve automated decision making. The DPO must be consulted if the school wishes to adopt a new process that includes automated decision making and profiling.

Responding to Data Subject Rights

The school will respond to all requests regarding data subject rights within one calendar month; the school reserves the right to apply a two-month extension for any requests that we deem complex, we will however inform the individual of any intention to extend within the first month.

All responses should confirm whether the school has been able to meet the request in full, part or not at all along with a clear explanation why. A copy of the relevant privacy notice will be included or referred to in all responses; the individual will also be informed of their right to complain to the ICO if they are unhappy with how the school has dealt with their request.

Recording the Rights of Individuals

To meet the UK-GDPR's accountability principle, the school will retain a log of all requests received regarding the rights of individuals. The log will include:

- Name & contact details of requester
- Date of request
- Whether the identity of the individual has been verified
- What has been requested

- Whether the request has been met in full, part or refused and the reasons why.
- Date of response.

Logs will typically be kept for a period of one year to account for the complaints process.

CCTV

Closed Circuit Television (CCTV) is in place at various locations across the Leo Kelly site to enhance security and aid in the prevention and detection of crime. The school comply with the ICO code of practice for the use of CCTV, in summary:

- A lawful basis for the use of CCTV has been established.
- DPIA's will be conducted and reviewed routinely to determine the privacy risks associated with the use of CCTV.
- Prominent signage will be placed at key areas that clearly informs individuals that CCTV is in place, the reasons why and details of the Data Controller.
- Access to the system is strictly limited to the designated staff member(s) identified in the DPIA; password protection is in place to restrict access to unauthorised users.
- Footage will not be released to individuals or third-party organisations such as the Police or Insurers without written authorisation from the headteacher and consultation with the DPO.

Please refer to the CCTV Policy for further information.

Artificial Intelligence (AI)

Artificial Intelligence (AI) and automated tools are utilised to enhance education, streamline administrative procedures, and support inclusive learning. The school takes a risk-based, secure approach to protect the rights and freedoms of staff and pupils when implementing AI technologies.

The school adheres to the following principles regarding AI usage:

- **Strict Data Limitations:** Staff, contractors, and volunteers must **never** input un-anonymised personal data, special category data (e.g., medical info), or sensitive safeguarding details into public or third-party generative AI platforms (e.g., ChatGPT) unless the tool has undergone a formal Data Protection Impact Assessment (DPIA) and received explicit approval from the DPO.
- **Pre-Deployment DPIA:** A DPIA must be conducted prior to introducing any AI tools that process personal data, evaluating privacy risks, ethical considerations, algorithmic bias, and security measures.
- **Human Oversight (No Automated-Only Decisions):** Meaningful human intervention must be applied to all outputs or recommendations produced by AI tools. No decision significantly impacting a pupil or staff member will be made solely via automated AI processing.
- **Transparency:** The school will clearly inform parents, pupils, and staff about how AI technologies are used within educational and administrative operations.

- **No AI Training on School Data:** The school will actively opt out of or prohibit suppliers from using school-supplied personal data to train public or proprietary AI models.
- **Anonymisation:** Personal data must be anonymised or pseudonymised prior to processing via approved AI platforms whenever reasonably practicable.

The school will continuously review AI systems in line with guidance from the Information Commission and the DfE.

Images
From time to time, we use images to celebrate achievements, promote the school and provide the community with an insight into school life; images also provide pupils and families with mementoes of their time at school. For the purposes of this policy, images refer to photographs and video footage processed by the school.

The use of images will typically be limited to the following:

- Internal displays
- Our website(s)
- Social media
- Local media (newspapers etc)
- Newsletters and circulars
- School photographers (annual photographs for parents)

The use of images for such purposes is optional and therefore consent will be sought prior to any images being taken or used. Consent will be sought in line with the process outlined in section 7.1 of this policy.

The school adopt the following approach:

- A log of consent will be kept and reviewed annually for pupil images; the relevant staff will have access to their school's respective log and will review prior to taking any images.
- All individuals will be verbally provided with an opportunity to step aside if they do not wish for their image to be taken.
- Images will not be accompanied by any further identifying features such as name unless explicit consent is in place.
- Alternative provisions will be available where possible to ensure non-consenting pupils are not discriminated against and feel included.
- Particular attention is given to pupils and staff whose identities should not be made public for safeguarding purposes prior to publicising any images.
- Images will be taken on school owned devices only; personal devices will not be used.

For the purposes of events, the school ask that parents and visitors refrain from taking images that include pupils other than their own child. Any images containing other pupils should not be shared publicly, for instance on social media. The school cannot control the use of images taken by third parties.

Please refer to the Safeguarding Policy for further information on our use of images.

Wearable Recording Devices & Smart Glasses

Wearable technologies with audio or visual recording capabilities (including smart glasses, hidden cameras, or body-worn recording devices) present specific privacy and safeguarding risks.

Staff, Contractors, and Visitors: Must not use smart glasses or wearable recording devices to capture images, video, or audio of pupils, staff, or visitors on school premises or during off-site school activities. Smart glasses with recording capabilities must have recording features disabled or be removed while on site.

Pupils: Pupils are strictly prohibited from bringing or wearing smart glasses with recording capabilities on school premises or during educational activities, in accordance with the school's Safeguarding and Mobile Technology policies.

Exceptions: Any legitimate recording using wearable tech for educational or administrative purposes must undergo a prior Data Protection Impact Assessment (DPIA) and receive formal approval from the Headteacher and DPO.

Data Protection by Design & Default

In order to achieve an effective data protection strategy, the school must integrate the key principles of the UK-GDPR into its organisational culture, structure and core business functions. To do this, the school will consider the privacy impacts and risks associated with processing prior to any data processing taking place (data protection by design):

- Ensuring a legitimate purpose has been established and a lawful basis met.
- Assessing what data is required and how we can best limit this to what is strictly necessary.
- Completing a DPIA on any high-risk processing activities or new technologies.
- Exploring less intrusive methods of processing.
- Using anonymisation and pseudonymisation where appropriate.

The school will take a proactive approach to ensure data protection lies at the heart of our organisation and remains ingrained within our culture (data protection by default):

- Appointing a DPO to oversee compliance; regular updates are provided to school leadership.
- Performing routine audits on both physical and technical security measures to identify any gaps in compliance and security.
- Integrating data protection into key policies and procedures and effectively communicating these with staff.
- Regularly training and briefing our staff on data protection and associated topics including cyber security to keep privacy and security relevant.
- Promoting transparency and an open culture to ensure staff are not afraid to report data breaches or notify us if they have concerns.

- Displaying visual aids around site as reminders of the key principles.
- Reviewing key documentation at intervals to ensure the content and our practices compliment one another and comply with the relevant legislation.

Data Breach Procedure
The school implements robust security measures to ensure as much as possible that data breaches do not occur. We do however realise that even the most secure of systems are not watertight, we have therefore implemented a procedure to help us deal with data breaches quickly and efficiently. In the unlikely event of a data breach, the school will follow the procedure set out below:

Notification

Upon discovering a data breach, staff will notify the Data Protection Officer (DPO) without undue delay. Data Processors and Joint Data Controllers must also notify the DPO of data breaches affecting school data.

Timing is of the essence; the sooner the school is notified of the breach the quicker we can work to mitigate the impacts. In addition, the school has a duty to report certain data breaches to the ICO within 72hours. We may also need to notify the affected individuals.

A list of key contacts will be readily available to staff to ensure the relevant person(s) can be contacted as soon as possible. Emergency contacts for the following individuals will be accessible:

- Data Protection Officer (DPO)
- Individual Responsible for Data Protection in the School
- ICT Lead (Cyber Related Breaches)

It is recommended that schools add contact details for the relevant departments at their respective local authority and policing services should a significant data breach occur.

Assessment & Review

The DPO will investigate the report to determine whether a data breach has occurred and advise the school on the immediate steps required to mitigate the breach. Steps will differ depending upon the nature of the breach.

An assessment will then be made by the DPO to ascertain the likely impacts of the breach, the severity of those impacts and the likelihood that they will occur. The DPO will discuss the assessment with the leadership team at the school or relevant school and a decision made on reporting.

Reporting

Manchester Hospital School

Any data breach that is likely to result in a high risk to an individual's rights and freedoms will be reported to the ICO within 72hours of discovery using the following link: https://ico.org.uk/for-organisations/report-a-breach/

If the full details are not yet known, the DPO will provide as much detail as possible to the ICO within the 72hour window. 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 school must also inform the affected individuals if there is a high risk to their rights and freedoms for instance if the breach is likely to lead to material, physical or mental harm. Individuals will be provided with an overview of the breach in writing, correspondence via telephone will be required for urgent situations. In addition to an overview of the breach, individuals will be provided with:

- The name and contact details of the DPO.
- A list of actions that have been taken to mitigate the breach and the adverse effects on them.
- Details on how to make a complaint to the ICO.

The school will consider support for the affected individuals where appropriate such as police involvement if the breach poses a threat to safety.

Data breaches that do not pose a high risk to an individual's rights and freedoms will be managed internally by the school.

Recording

All data breaches no matter the severity will be kept on the school data breach log; the school encourages the reporting and logging of near misses to improve security measures. A breach log is in place with access limited to staff on a 'need to know' basis, the log includes:

- Breach reference number
- Date of breach
- Staff member responsible
- No of individuals affected.
- Description of breach
- How it was discovered
- Categories of data affected.
- Potential consequences
- Actions taken.
- Whether it is reportable to the ICO and affected individuals (including dates reported)

The DPO will also record the assessment and decision-making process for high-risk reportable breaches.

Review

Manchester Hospital School

Once the school has taken the necessary actions to mitigate the breach as much as possible, measures to prevent the breach re-occurring will be discussed and implemented by the DPO and relevant staff members.

The school will take steps to review and monitor the impact of the breach moving forward. This may include online searches to ensure data has not been publicised and corresponding with the affected individuals to monitor any impacts of the breach.

School staff will support the DPO where necessary throughout the data breach procedure.

Storage of Records
The school will store records securely and in an organised manner taking into account the following:

- Records need to be secure, yet accessible for use by the relevant staff members. Access controls must be in place to ensure staff only access what they need to.
- Records need to be searchable to ensure information requests can be met efficiently; a uniform method of addressing individuals is recommended to ensure records can be easily collated upon request.
- Records must be stored in chronological order to support their retention period; records ready for deletion should be identifiable.
- Staff are encouraged not to use their email account as a system for storage; key records should be filed on recommended databases only.
- The location of records should be known and logged for traceability; if a staff member leaves, the departmental lead will need to make records accessible to their replacement.

Disposal of Records
Once records are due to come to the end of their retention period, a review will take place to assess whether or not records are still required or if they can be securely destroyed. Particular care should be taken to review safeguarding and personnel files to account for any ongoing or likely investigations and claims.

Electronic records will be securely deleted from the school server and remote platforms taking into consideration any recycle bins and temporary deletion folders. Automated deletion will be applied for any electronic records that do not require a manual review prior to disposal. The school ICT department will be consulted to ensure records are fully cleansed and removed from the system(s).

Physical records will be securely shredded on site by school staff or via carefully selected shredding partners who provide adequate proof of destruction.

A general log will be kept outlining when data sets have been destroyed.

Training
All staff are subject to a data protection briefing upon induction and receive routine training on both data protection and cyber security. The school will issue staff with routine briefings at intervals to ensure the key data protection principles remain relevant.

Data protection will form a key part of staff continual professional development; a record of all training is kept by the school.

Monitoring
This policy will be reviewed every three years or sooner should a significant change in legislation or data processing activities occur. The Data Protection Policy is a statutory policy that should be reviewed by the governing board.

The policy and any changes will be communicated to all school staff.

Complaints
If you have questions, concerns, or wish to make a complaint about how the school handles your personal data, you have the right to lodge a formal complaint.

Internal Complaints Procedure:

In accordance with statutory requirements, individuals must first submit their complaint directly to the school to allow for an internal investigation and resolution before escalating to the supervisory authority:

1. **Submit Complaint:** Contact the school office or the Data Protection Officer (DPO) in writing, detailing the nature of your concern.
2. **Investigation & Response:** The DPO, alongside the school leadership team, will investigate the matter and provide a formal written response outlining the findings and any remedial action taken without undue delay (and within 30 calendar days).

Escalation to Regulator: If you remain unsatisfied with the school's final response, or if the school fails to address your complaint appropriately, you have the right to lodge a complaint with the **Information Commissioner's Office (ICO) / Information Commission**:

- **Website:** https://ico.org.uk/make-a-complaint/

- **Telephone:** 0303 123 1113
- **Address:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Appendix 1: Useful Data Protection 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
Biometric Data	The automated recognition of individuals based on their biological and behavioural characteristics; examples include fingerprint and facial recognition scanning.
Artificial Intelligence	The theory and development of computer systems able to perform tasks normally requiring human intelligence.

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.
Information Commissioners Office (ICO)	Governing Body for data protection in the UK.