MANOR
MULTI ACADEMY TRUST

Policy Document for: Data Protection (UK GDPR)

Approved by Directors: Jan 2023

Due for Review: Jan 2024

Contents

Statement of intent

Manor Multi Academy Trust is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation 2021 (UK GDPR 2021). We live in a data driven world and we would only use data as one would reasonably expect. Personal data information is kept securely and it helps our Trust and Schools run efficiently and effectively.

The Trust may, from time to time, be required to share personal information about its staff, pupils and families with other organisations, such as Local Authorities, educational bodies and schools, social services and NHS.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the trust complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and Manor Multi Academy Trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

With the adequacy decision adopted under the UK GDPR, the Commission confirms that the UK offers an adequate level of protection for personal data, known as the "adequacy agreement". As a consequence, the continued free flow of personal data between the EU and UK is guaranteed at least until 27 June 2025, unless extended.

Associated Legal frameworks

This policy has due regard to legislation, including, but not limited to the following:

- Data Protection Act 1998, 2018 & UK GDPR (1st Jan 2021)
- Freedom of Information Act 2000
- Education Act 2011
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: · Name (including initials) · Identification number · Location data · Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity
Special categories of personal data	Personal data which is more sensitive and so needs more protection, 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 · Gender and 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.

Applicable data

For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g., key coded.

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

Principles

In accordance with the requirements outlined in the UK GDPR, personal data will be:

- ✓ Processed lawfully, fairly and in a transparent manner in relation to individuals.
- ✓ Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- ✓ Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- ✓ Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- ✓ Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- ✓ Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

Accountability

Manor Multi Academy Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

- ✓ The trust will provide comprehensive, clear and transparent privacy policies.
- ✓ Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.
- ✓ Offer annual staff training MAT wide (all schools and central teams)

Internal records of processing activities will include the following:

- ✓ Name and details of the organisation
- ✓ Purpose(s) of the processing
- ✓ Description of the categories of individuals and personal data
- ✓ Retention schedules

- ✓ Categories of recipients of personal data
- ✓ Description of technical and organisational security measures
- ✓ Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- ✓ Data minimisation.
- ✓ Pseudonymisation.
- ✓ Transparency.
- ✓ Allowing individuals to monitor processing.
- ✓ Continuously creating and improving security features.
- ✓ Data protection impact assessments will be used, where appropriate.

Data Protection Officer role (DPO)

The appointed DPO will:

- Inform and advise the trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the trust's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to trusts.

The DPO will report to the highest level of management at the trust, which is the Chief Executive Officer (CEO). The DPO will operate independently and will not be dismissed or penalised for performing their task Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations.

Data Protection Officer Contact:

In the event of an individual requiring a Data related service such as a Freedom of Information or Subject Access request, please contact our MAT Data Protection Officer. Appendix 1 offers examples of the DPO role activities.

Name:	Neil Beards
Role:	MAT Data Protection Officer
Areas of responsibility	Manor Multi Academy Trust & all MAT Schools
Contact Number:	01902 556460
Contact Email:	dpo@manormat.com
ICO Registration:	https://ico.org.uk/ESDWebPages/Entry/ZA174023

Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
    - Compliance with a legal obligation.
    - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - For the performance of a contract with the data subject or to take steps to enter into a contract.
    - Protecting the vital interests of a data subject or another person.
    - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject unless reliance on consent is prohibited by UK law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of UK law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. On occasion there may be a method of "opt-out" consent which people will be informed of.

Where consent is given, a record will be kept documenting how and when consent was given. People must confirm that the have had consent from a third party if giving personal information on their behalf, e.g. Emergency contact.

The trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

Consent can be withdrawn by the individual at any time. The instruction must be clear and recorded by the individual to the Trust and / or School.

The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

The rights

To be informed:

The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

The right of access

Individuals have the right to obtain confirmation that their data is being processed.

Individuals have the right to submit a "Subject Access Request" (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The trust will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the trust will ask the individual to specify the information the request is in relation to.

The right to rectification

It is the individual's responsibility to inform the Trust and / or School of any changes to personal or sensitive information. The Trust and it's Schools should request this annually from all associated people.

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the trust will inform them of the rectification where possible.

Where appropriate, the trust will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the trust will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

The trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress the trust's processing of personal data if there is a reasonable reason to do so.

In the event that processing is restricted, the trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the trust has verified the accuracy of the data
- Where an individual has objected to the processing and the trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

If the personal data in question has been disclosed to third parties, the trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The trust will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form.

The trust will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Manor Multi Academy Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the trust will consider whether providing the information would prejudice the rights of any other individual.

The trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their situation in order to exercise their right to object.

- Where the processing of personal data is necessary for the performance of a public interest task, the trust is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the trust will offer a method for individuals to object online.

Privacy by design and privacy impact assessments

The trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the trust has considered and integrated data protection into processing activities. The Trust and schools will inform the DPO of any changes or required DPIA's.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Manor Multi Academy Trust's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be used for more than one project, where necessary.

High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

The trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The DPO and senior MAT school leaders will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the trust becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the trust will notify those concerned directly.

A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the Data Protection Officer (DPO)
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

Failure to report a breach when required may result in a fine, as well as a fine for the breach itself. Appendix 3 references some examples that may be of use to identify what may constitute as a data breach.

Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up on and off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks or removable media will not be used to hold personal information unless they are password-protected and fully encrypted. Removable data storage will be phased out during Spring Term 2023 on all Academy Trust devices.

All Server storage whether locally saved or cloud-based systems the Trust use has strict permissions set for access to authorized individuals.

All technology devices that access or save any personal data are password-protected or pin coded to protect the information on the device in case of theft.

Where possible, the trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not use their personal laptops or computers for trust purposes where personal data is used/concerned.

All necessary members of staff are provided with their own secure login and password. Two-factor authentication is enabled for all staff user accounts from Spring Term 2023.

Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices

under lock and key. The person taking the information from the trust premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the trust containing sensitive information are supervised at all times.

The physical security of the trust's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Manor Multi Academy Trust takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data. Appendix 2 refers to several measures we use to minimise the risk and impact of data breaches.

Publication of information

Manor Multi Academy Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Classes of information specified in the publication scheme are made available quickly and easily on request.

Manor Multi Academy Trust will not publish any personal information, including photos, on its website without the prior consent and permission of the affected individual.

When uploading information to the trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

CCTV and photography

The trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via local school notice boards and signs.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept up to a maximum of 90 Days for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing restricted access. This information depending on the circumstance may be shared with relevant authorities such as the Local Authority and Emergency services.

The trust will always indicate its intentions for taking photographs of pupils and will acquire the appropriate consent before publishing them.

If the trust wishes to use images/video footage of pupils in a publication, such as the trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR. Further details about the CCTV Policy can be obtained from the website http://www.manormat.com/governance/gdpr

Directors, Trustees and Governors

The Trust accepts that Directors, Trustees and Governors will access some confidential information which may include personal and highly sensitive information within the organisation via their own personal devices. This group must have in place a secure pin or password for their personal device and ensure that this accessible information is protected and not shared with any other persons. We advise against downloading the information to any personal device but encourage to delete as soon as possible if this is the only option to them. All associated persons within these groups are issued with an organization @manormat.com account which must be used over any personal email account. The Trust will continue to improve methods and work on practical solutions to avoid any possible compromise situations to protect the individuals and Trust. The Trust uses Governor Hub and Microsoft Teams to achieve secure storage solutions when sharing information.

Data retention

Data will not be kept for longer than is necessary or lawfully required. The Trust operates and retention schedule which is publicly published in line with standard UK education organisations.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded, and electronic memories securely cleaned or destroyed, once the data should no longer be retained.

DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

ICO Contact Information:

If you feel we are not responding effectively with your request it may be in your interest to make contact with the Information Commissioner's Office who may be able to advise you further. In any instance please give us the opportunity to deal with your request within the timeframes allowed.

Information Commissioner's Office · Phone

Wycliffe House Water Lane, Wilmslow SK9 5AF

0303 123 1113

https://ico.org.uk/

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO via email dpo@manormat.com
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - ✓ Lost
  - ✓ Stolen
  - ✓ Destroyed
  - ✓ Altered
  - ✓ Disclosed or made available where it should not have been
  - ✓ Made available to unauthorised people
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the HeadTeacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary and the DPO should take external advice when required (e.g. from IT providers). (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The DPO will work out whether the breach must be reported to the ICO using the self-assessment tool. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - ✓ Loss of control over their data
  - ✓ Discrimination
  - ✓ Identify theft or fraud
  - ✓ Financial loss
  - ✓ Unauthorised reversal of pseudonymisation (for example, key-coding)
  - ✓ Damage to reputation
  - ✓ Loss of confidentiality
  - ✓ Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored the schools spreadsheet on individual servers.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
  - ✓ A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - ✓ The name and contact details of the DPO
  - ✓ A description of the likely consequences of the personal data breach
  - ✓ A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours.
- The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - ✓ A description, in clear and plain language, of the nature of the personal data breach
  - ✓ The name and contact details of the DPO
  - ✓ A description of the likely consequences of the personal data breach
  - ✓ A description of the measures that have been, or will be, taken to deal with the data breach
  - ✓ and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - ✓ Facts and cause
  - ✓ Effects
  - ✓ Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - ✓ Records of all breaches will be recorded on the schools spreadsheet.
- The DPO and school leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Appendix 2: Actions to minimise the impact of data breaches

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

- Sensitive information being disclosed via email (including safeguarding records)
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Appendix 3: Examples of Data Breaches

- Non-anonymised pupil exam results or staff pay information being shared with governors
- The sender must attempt to recall the information as soon as they become aware of the error
- The governors must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the information for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the information, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The individual must inform the School Leader and the ICT department as soon as possible.
- The School leader will follow the same procedure for personal data breaches above.
- The school's cashless payment provider being hacked and parents' financial details stolen

The DPO will report the breach and follow the same procedure for personal data breaches above.