THE MANOR TRUST

Data Protection Policy

Agreed and approved by	The Trust Board
Date approved	March 2025
Date to be reviewed	March 2027
Version	1

1.0 Overview 3
2.0 Scope and Applicability 3
3.0 General Policy 3
3.1 Objectives 3
3.2 ICO Registration 5
3.3 Introduction to the UK GDPR 5
3.4 Data Protection Principles 5
3.5 External Data Transfers 7
3.6 Safeguards 8
3.7 Data Subjects' Rights 8
3.8 Complaints 8
3.9 Consent 8
3.10 Security of Data 10
3.11 Rights of Access to Data - Subject Access Request (SAR) 11
3.12 Retention and Disposal of Data 13
3.13 Security Incidents / Personal Data Breach Procedure 13
4.0 Roles and Responsibilities 14
5.0 Compliance 15
6.0 Risk Management 15
7.0 References 15
8.0 Definitions 15
9.0 Review 16
Appendix 1 - Data Breach Procedure 17
Appendix 2 - Subject Access Request (SAR) Procedure 23
Appendix 2a - Subject Access Request Form 28
Links with other policies 32

1.0 Overview

We are The Manor Trust (“the Trust”), a Multi-Academy Trust (MAT) based in Croydon. Our address is The Manor Trust, Norbury High School For Girls, Kensington Avenue, Thornton Heath CR7 8BT. We currently oversee two academies:

- Kensington Avenue Primary School
- Norbury High School For Girls

The purpose of this policy is to ensure that The Manor Trust is committed to compliance with all relevant data protection laws in respect of personal data and to the ‘rights and freedom’ of individuals whose information is collected. The Trust intends to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR). To that end, the Trust has developed, implemented, maintains and continuously improves data protection policies and procedures.

2.0 Scope and Applicability

The Trust is the Data Controller for the purposes of data protection law for all the personal data processed at Kensington Avenue Primary School and Norbury High School For Girls under the UK General Data Protection Regulation (UK GDPR).

This policy applies to all Trust staff including staff at each school, trustees, members, governors, temporary staff and contractors. Compliance with data protection legislation is the responsibility of all members of the Trust who process personal information and failure to comply with this policy may lead to disciplinary action.

3.0 General Policy

3.1 Objectives

The Trust is committed to complying with data protection legislation and good practice including:

- Processing personal information only where this is strictly necessary for legitimate purposes
- Collecting only the minimum personal information required for these purposes and not processing excessive personal information
- Providing clear information to individuals about how their personal information will be used and by whom
- Only processing relevant and adequate personal information
- Processing personal information fairly and lawfully
- Maintaining an inventory of the categories of personal information processed by the Trust
- Keeping personal information accurate and, where necessary, up to date
- Retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate purposes
- Respecting individuals’ rights in relation to their personal information including their right of subject access

- Keeping all personal information secure
- Only transferring personal information outside the United Kingdom in circumstances where it can be adequately protected
- The application of the various exemptions allowable by data protection legislation

3.2 ICO Registration

3.2.1 The Trust has notified the Information Commissioner's Office (ICO) that it is a Data Controller and that it processes certain information about Data Subjects. Each school within the MAT has identified all the personal data that it processes and this is contained in the Record of processing activities (ROPA).

3.2.2 A copy of the ICO Registration is retained by the CEO and is available to view on the ICO website.

3.2.3 The ICO registration is renewed before expiry.

3.2.4 The Trust's nominated people are responsible, each year, for reviewing the details of registration in the light of any changes to the MAT's size or structure.

3.3 Introduction to the UK GDPR

The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK and supersedes the Data Protection Act 1998. It is a national law which sits alongside the UK GDPR and which, from 1st January 2021, replaces the European Union's General Data Protection Regulation due to the UK's exit from the European Union.

The purpose of the UK GDPR is to protect the "rights and freedoms" of living individuals, to ensure that personal data is not processed without their knowledge and that it is processed lawfully.

The UK regulator for Data Privacy is the ICO. The ICO provides a 'Guide to the UK GDPR' which is used by the Trust's Data Protection Officer to understand the details of the regulation.

3.4 Data Protection Principles

All processing of personal data must be done in accordance with the following data protection principles of the UK GDPR. The Trust's policies and procedures are designed to ensure compliance with them.

<u>Personal data must be processed lawfully, fairly and transparently.</u>

The UK GDPR stipulates the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language commonly in the form of a privacy notice.

The specific information that must be provided to the data subject must as a minimum include:

3.4.1 The contact details of the School/Trust (as applicable)

3.4.2 The contact details of the DPO

3.4.3 The purposes of the processing for which the personal data are intended as well as the legal basis for the processing

3.4.4 Who the personal data will be shared with

3.4.5 The period for which the personal data will be stored

3.4.6 The existence of the data subject rights

3.4.7 The categories of personal data concerned

3.4.8 If the data is transferred out of the UK

3.4.9 Any further information necessary to guarantee fair processing

Personal data can only be collected for specified, explicit and legitimate purposes

3.4.10 Data obtained for specified purposes must not be used for a purpose that differs from those documented in the Record of processing activities (ROPA) and stipulated in the Privacy Notices.

Personal data must be adequate, relevant and limited to what is necessary for processing

3.4.11 The Trust is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

3.4.12 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the school's head teacher or nominated contact.

3.4.13 The Trust will review data collection methods on a regular basis to ensure that collected data continues to be adequate, relevant and not excessive.

3.4.14 If data is given or obtained that is excessive or not specifically required by the Trust's documented procedures, the Trust's nominated contact is responsible for ensuring that it is securely deleted or destroyed in line with the Trust's retention schedules.

Personal data must be accurate and kept up to date

3.4.15 Personal Data that is processed must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.

3.4.16 The Trust's nominated contacts are responsible for ensuring that all staff members are trained in the importance of collecting accurate data and maintaining it.

3.4.17 It is also the responsibility of individuals to ensure that data held by the school is accurate and up to date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.

3.4.18 Data subjects should notify the Trust of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Trust to ensure that any notification regarding change of circumstances is noted and acted upon within 1 month.

3.4.19 The Trust is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

3.4.20 Each school's head teacher and nominated contact will review all the personal data maintained by the school on a regular basis, by reference to the Record of Processing Activities (ROPA), and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with the data retention schedule.

3.4.21 The Trust and nominated contacts are responsible for making appropriate arrangements, in the event third party organisations are passed inaccurate or out-of-date personal information, that any inaccurate and/or out-of-date personal information is not to be used to inform decisions about the individuals concerned and for passing any correction to the personal information to the third party required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

3.4.22 Where personal data is retained beyond the processing date, it will be held securely in order to protect the identity of the data subject in the event of a data breach.

3.4.23 Personal data will be retained in line with the Trust's Records Retention Schedule and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

Personal data must be processed in a manner that ensures its security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Data held by the Trust is secure, controlled and managed and in compliance with UK GDPR.

Security controls may be subject to audit and review by independent auditors.

The controller shall be responsible for, and be able to demonstrate compliance with accountability

The UK GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the UK GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs, comply with requirements for prior notifications, or approval from the ICO and appoint a DPO.

3.5 External Data Transfers

Personal data shall not be transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the United Kingdom is prohibited unless one or more of the specified safeguards or exceptions apply.

3.6 Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

3.6.1 The nature of the information being transferred

3.6.2 The country or territory of the origin, and final destination, of the information

3.6.3 How the information will be used and for how long

3.6.4 The laws and practices of the country of the transferee, including relevant codes of practice and international obligations

3.6.5 The security measures that are to be taken as regards the data in the overseas location

3.7 Data Subjects' Rights

Data subjects have the following rights regarding personal data that is recorded about them:

3.7.1 The right to be informed

3.7.2 The right of access

3.7.3 The right to rectification

3.7.4 The right to erasure

3.7.5 The right to restrict processing

3.7.6 The right to data portability

3.7.7 The right to object

3.8 Complaints

In the first instance Data Subjects who wish to make a complaint about how their personal information has been processed may raise this with the Trust.

If Data Subjects are not satisfied with the outcome of their complaint or the way in which it has been handled, they also have the right to complain directly to the ICO.

3.9 Consent

The Trust understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

The Trust understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For special category data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and special category data is obtained routinely by the Trust using standard consent documents e.g. when a new member of staff signs a contract of employment or during induction for participants on programmes.

Where the Trust/School provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

As part of day-to-day school activities, employees of the Trust/School may take photographs and record images of pupils but will obtain consent from parents/carers, for those under the age 13, beforehand to ensure any photographs and videos taken can only be used for purposes consent has been given for. Pupils aged 13 years and over can provide their own consent. Consent forms will clearly explain how the photograph and/or video will be used.

Uses may include:

- Internal use - within school on notice boards, including digital displays and posters, newsletters
- External use - in school magazines/publications, brochures/prospectus, leaflets, school newsletters, on banners / advertising boards
- Third parties - external agencies such as school photo/videographers, newspapers, campaigns, TV/radio/digital broadcasters
- Online – Trust/School websites, social media channels and pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. Where pictures are published, we will only use first names and will not include any other personal information to ensure the child cannot be identified. If full names are requested, we will seek explicit consent from a parent/ carer or the pupil themselves if they are aged 13 years or above, before proceeding.

<u>Use of CCTV</u>

The Trust uses CCTV around our sites (internal and external) for the purpose of ensuring the

safety and well-being of Trust staff, pupils and visitors and to monitor activities around school premises, entrances, car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, in compliance with the regulatory requirements, in particular, UK GDPR and the Data Protection Act 2018 (DPA). As per UK GDPR, permission or consent is not required for recording, but clear signage is displayed in all relevant areas to inform data subjects about the use of CCTV and the potential collection of personal data

.

3.10 Security of Data

All staff are responsible for ensuring that any personal data which the Trust/School holds and for which they are responsible is kept securely and is not under any condition disclosed to any third party unless that third party has been specifically authorised by the Trust to receive that information and has entered into a confidentiality agreement.

Any third parties working with or for the Trust, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the Trust without having first entered into an agreement which imposes on the third party obligations no less onerous than those to which the Trust is committed and which gives the Trust the right to audit compliance with the agreement.

All personal data should be accessible only to those who need to use it. The Trust will form a judgement based upon the sensitivity and value of the information in question, but personal data must be kept:

3.10.1 In a locked room with controlled access
3.10.2 In a locked drawer or filing cabinet
3.10.3 If computerised, encrypted / password-protected
3.10.4 Encrypted if stored on mobile/removable devices

Care must be taken to ensure that PC screens and terminals are not visible except to authorised members of Trust staff.

Manual records are not to be left where they can be accessed by unauthorised personnel and may not be removed from Trust premises without explicit authorisation.

Personal data will only be deleted or disposed of in line with the Trust's Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Storage drives of redundant PCs and mobile devices are to be removed and immediately securely destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site and appropriate security controls implemented.

Security controls may include:

3.10.5 Data encryption
3.10.6 Password or PIN protected data
3.10.7 Secure storage device
3.10.8 Secure remote access to the data

3.10.9 Not working in an environment that is not secure or safe such as an internet cafe

3.10.10 Not keeping laptops or paper records overnight in a vehicle

3.11 Rights of Access to Data - Subject Access Request (SAR)

Data subjects have the right to access any personal data (i.e. data about them) which is held by the Trust in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Trust, and information obtained from third parties about that person. SARs across the Trust are dealt with as described in the SAR Procedure (Appendix 2).

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request (SAR). Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 and over are generally considered to have the maturity to understand their rights under the UK GDPR, including the implications of making a Subject Access Request (SAR). Therefore, when a SAR is made by a child aged 13 and over, we will assess their understanding of the request and their ability to exercise their rights independently. In cases where the child is deemed capable of understanding, their consent may be required. For SARs made by parents or carers of children aged 13 and over, we may still require the express consent of the pupil, depending on their maturity and understanding. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

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

When responding to requests, we:

3.11.1 May ask the individual to provide 2 forms of identification

3.11.2 May contact the individual via phone to confirm the request was made

3.11.3 Will respond without delay and within 1 month of receipt of the request

3.11.4 Will provide the information free of charge

3.11.5 May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

If the request is unfounded or excessive, we may refuse to act on it. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

If we refuse a request, we will tell the individual why, and inform them of their right to complain to the ICO.

Disclosure of data

The Trust must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies and, in certain circumstances, the police.

All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the Trust's business.

We may not disclose information if it:

3.11.6 May cause serious harm to the physical or mental health of the pupil or another individual.

3.11.7 Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interest.

3.11.8 Is contained in adoption or parental order records.

3.11.9 Is given to a court in proceedings concerning the child.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO. The regulations allow for some exemptions. These too should be discussed with the DPO.

3.12 Retention and Disposal of Data

Personal data may not be retained for longer than it is required. For example, once a member of staff has left the Trust, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. The Trust's Records Management and Retention Policy will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion). We may also use a third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and secure disposal practices.

3.13 Security Incidents / Personal Data Breach Procedure

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. However, in the event of a suspected data breach, we will follow the internal data breach procedure as well as external breach reporting procedures. These are detailed in the Security Incident Procedures, set out in Appendix 1.

All security incidents are recorded by the Trust and all staff have been trained to recognise both a security incident and a personal data breach.

The Trust in conjunction with anyone involved in the finding or causing of a breach, or potential breach, notifies the DPO of all incidents as soon as practical after the incident has been discovered.

When a personal data breach has occurred, the Trust in conjunction with the DPO will establish the likelihood and severity of the resulting risk to individual's rights and freedoms. If there is likely

that there will be a risk, the ICO must be notified. The DPO will report serious data breaches within 72 hours of the incident to the ICO.

The UK GDPR states “A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

Any serious breach of data protection legislation will be dealt with under the Trust’s disciplinary policy and may also be a criminal offence, in which case the matter will be reported to the Information Commissioner’s Office (ICO) or police.

4.0 Roles and Responsibilities

- The Board of Trustees has overall responsibility for ensuring schools comply with all relevant data protection obligations
- The head teacher of a school acts as representative of the Data Controller on a day-to-day basis, responsible for developing and encouraging good information handling practices
- The Data Protection Officer (DPO), a role specified in the UK GDPR, is accountable for ensuring that compliance with data protection legislation and good practice can be demonstrated

  The DPO for The Manor Trust is:
  Data Compliance Service - The Education Space
  3rd Floor, Boardman House. 64 Broadway, London E15 1NT
  dpo@theeducationspace.co.uk

This accountability includes:

1. Development and implementation of the UK GDPR as required by this policy; and
2. Security and risk management in relation to compliance with the policy.

- The Trust’s nominated person / DP Lead(s) have been appointed to take responsibility for schools’ compliance with this policy on a day-to-day basis and, in particular, have direct responsibility for ensuring that a school complies with the UK GDPR, as do staff in respect of data processing that takes place within their area of responsibility
- The head teacher of each school and that school’s nominated person have specific responsibilities in respect of procedures and will act as the first point of call for staff seeking clarification on any aspect of data protection compliance
- A school's nominated person will be the conduit between the school and the DPO for

security incident reporting

- The Trust will ensure appropriate data protection training is provided for all staff
- Staff are responsible for ensuring that any personal data supplied by them to the Trust, and that is about them, is accurate and up to date

5.0 Compliance

Compliance is mandatory and will be enforced for all employees, vendors and contractors.

Non-compliance with this and other policies may be subject to disciplinary action, up to and including dismissal.

6.0 Risk Management

Risk management for the both schools is set out in the Risk Register.

7.0 References

None

8.0 Definitions

SARs - Subject Access Requests

UK GDPR - UK General Data Protection Regulation

ICO - Information Commissioner's Office

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK law, the controller or the specific criteria for its nomination may be provided for by UK law. The Trust is a data controller.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – The UK GDPR does not define the age at which a person is considered to be a child. The processing of personal data of a child under 13 years of age in relation to online services is only lawful if parental or guardian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

9.0 Review

This policy will be reviewed and updated on a regular basis, not to exceed 24 months and shared with the Trust board.

THE MANOR TRUST

Data Breach Procedure

Approved by:	
Data Approved	
Date to be Reviewed	
Version	

This procedure has been produced based on current UK General Data Protection Regulations (UK GDPR) information produced by the Information Commissioner's Office (ICO) on guidance on personal data breaches. As further updates are released this procedure may be updated to reflect the changes.

Data Breach Procedure for The Manor Trust, Norbury High School For Girls and Kensington Avenue Primary School

Introduction

This procedure applies to all personal and sensitive data held by the Trust, Norbury High School For Girls and Kensington Avenue Primary School inclusive of all school staff, temporary staff, governors, trustees, members, volunteers and contractors, referred to hereinafter as 'staff'.

The Manor Trust is the data controller for both schools and combined, a large amount of personal and sensitive data is held and processed. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

All staff are required to be aware of and follow this procedure in accordance to reporting a security incident involving data. This procedure outlines the protocol for reporting any such incident, and also to the internal data protection leads and external Data Protection Officer (DPO) for the school.

Purpose

This breach procedure sets out the course of action to be followed by all staff if a personal data protection breach takes place regardless of how.

Identifying a Breach

All staff have a responsibility to identify and record any security incidents relating to the loss (temporary or permanent) of Trust data. The recording of security incidents shall take place irrespective of how the incident occurred and who was responsible.

Prompt action may be necessary to reduce the potential impact of an incident, so there may be times when an incident is resolved before it is recorded. If this occurs, a breach incident form should be completed as soon as possible after the event.

Reporting and Managing a Data Breach

If you become aware of or suspect a personal data breach that meets the outlined criteria, the staff member or data processor must;

- Immediately complete the online incident reporting form in the first instance which can be requested from the DP Lead, found below (link/url) or on the school website under GDPR
- The staff member should notify the relevant DP Lead as soon as possible to ensure all correct measures have been taken.

The Manor Trust Security Incident and Data Breach Form (Click link) or enter https://forms.gle/UMtuVQybTd78hDRTA into the URL address bar.

- Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The DPO will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DP Lead(s).
- The DPO will investigate the report to determine whether a breach has occurred, the severity, and the necessary actions to be taken. To help 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 and the level of risk associated
    - Contained internally
    - Steps taken to minimise impact
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non- material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The DPO will correspond with the reporter in the first instance, and will alert the nominated contact for the school, the head teacher of the school, CEO of the Trust and the chair of governors if required / where applicable of the incident.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will 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 on the school's server within a DPO account - Access to this information is shared with the Trust, head teachers, CEO and chair of governors by way of reports.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website (https://ico.org.uk/for-organisations/report-a-breach/) 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.
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - 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)
    - The DPO and Trust representative will meet to review severe cases. This meeting will happen as soon as reasonably possible.

The DPO for The Manor Trust is;

Data Compliance Service -The Education Space
3rd Floor, Boardman House. 64 Broadway, London,E15 1NT

dpo@theeducationspace.co.uk

Data Subject Notification

Where applicable, the school, person(s) responsible for the breach or DPO will notify data subjects of the personal data breach without undue delay. Data subjects will be provided with the following:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects
- A full report can also be provided in a written, clear and legible format.

Record Keeping

All records and notes taken during the identification, recording, investigation and notification of the security incident are recorded and authorised by the DPO and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed regularly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

Actions to minimise the impact of data breaches of Personal and sensitive information being shared via digital transfer /email (including safeguarding records)

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.

- *Use of secure reputable transfer platforms that safeguard and encrypt data; inclusive of secure links with access restrictions, tracking and password protecting.*
- *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 DP Lead as soon as they become aware of the error*
- *Where applicable, If the sender is unavailable or cannot recall the email for any reason, the DP Lead will ask the ICT department to recall it if possible*
- *An email delay on sent items will be set to allow sending to be cancelled or the email altered before being sent.*
- *In any cases where the recall is unsuccessful, the DP Lead 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 DP Lead will make reasonable efforts to obtain written confirmation from all recipients of the data, confirming their compliance with this request.*
- *The DP Lead will conduct an internet search, where feasible, to check if the information has been made public. If identified, we will take appropriate steps to request its removal from the publisher, website owner, or administrator.*
- *A mandatory email disclaimer, provided by the ICT team, should be added to all staff email accounts in accordance with the staff AUP. This disclaimer supports and demonstrates GDPR obligations by ensuring the protection and confidentiality of personal data and reminding staff of their responsibility to handle sensitive information appropriately.*

Disclaimer: *'This email and any attachments to it may be private/confidential and are intended solely for the use of the individual to whom it is addressed. It may also be privileged or otherwise protected by work product immunity or other legal rules If you have received this email in error, please notify the sender immediately by e-mail or telephone and delete the e-mail from any computer. You must neither take any action based upon its contents, nor copy or show it to anyone.'*

The Manor Trust

Subject Access Request (SAR) Procedure

Approved by:	Local Governing Body
Date Approved	
Date to be Reviewed	
Version	

Overview

Under the General Data Protection Regulation (GDPR), data subjects are entitled to exercise their right of access to any personal data about themselves and if the request is valid, be provided with the requested information in an easy to access format, free of charge, within one month of the request (excluding educational records, which is 15 school days) of the request The right of individuals to access their personal information can be fulfilled via a subject access request (SAR).

Scope & Applicability

This procedure applies to all personal data processed by The Manor Trust across its academies, including Kensington Avenue Primary School and Norbury High School for Girls and applies to all staff who deal with SARs. Paper and electronic records must both be considered when fulfilling a SAR.

The request may be received from a parent, a pupil or a third party such as a solicitor. Representatives will need to provide proof of consent to act on behalf of a data subject's request.

Responsibilities

All staff across the Manor Trust are responsible for ensuring that any request for information they receive is dealt with in line with UK GDPR by following this procedure.

All staff have a responsibility to recognise a request for information and ensure the Headteacher and DP Lead for the school that receives a SAR is notified within two working days.

The school's nominated person and staff associated with the data subject request are responsible for coordinating all SARs, the application and effective working of this procedure and for reporting to the data subject.

Receiving / Identifying SAR requests

SARs may be received via a variety of methods including email, website contact forms, social media, letter, telephone or in person. Any request from a data subject for personal information will be treated as a SAR and this request must be reported to the Headteacher , The Trust's nominated person / data protection lead per establishment (see below for email contact).

DP Lead for The Manor Trust: Markieu Hayden: dplead@themanortrust.org.uk

DP Lead for Norbury High School for Girls: Petra Lindsay: dplead@nhsg.org.uk

DP Lead for Kensington Avenue Primary: Dean Dumont: dplead@kaps.croydon.sch.uk

If a member of staff, permanent or contracted receives a request in person, it is good practice to acknowledge the data subjects request but redirect them to the school office to receive further information on registering their request – A SAR form (Appendix A) can then be offered to them to complete or downloaded from the trust/school website - The form is not mandatory but it is recommended to help clarify the extent and scope of the request.

General Policy

The UK GDPR specifies two reasons for granting individuals access to their personal data: to ensure they are aware of how their data is being used and to verify the lawfulness of its

processing.

The Trust/School will in most cases provide a copy of the information free of charge.

The Trust/School will act on SARs without undue delay, and at the latest within one month of receipt.

The time limit should be calculated from the day after the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

This period may be extended by two further months where requests are complex or numerous, with notification to the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the trust/school can:

- Charge a reasonable fee taking into account the administrative costs of providing the information
- Refuse to respond

When a request is refused, the Trust/School must explain why to the individual, informing them of their right to complain to the Information Commissioner's Officer (ICO) and to a judicial remedy without undue delay and at the latest within one month.

Whilst the Trust/School cannot insist upon the completion of a SAR form (See Appendix 2a for our SAR form), data subjects should be directed to complete and submit a form as this will aid the fulfilment of the request.

Verification of Identity

The requester should be asked to verify their identity by providing acceptable documentation. One item from list A and one item from list B is required.

List A	List B
Photographic proof of identification	Proof of address
Passport	Bank Statement
Photographic Driving License	Utility Bill

The requester should present the identification documents in person to the school promptly. The documents will be verified and the request will move to the fulfilment stage.
Under no circumstances should information be disclosed to anybody prior to their identity being verified.

Fulfillment of Request

The Trust's/School's nominated person will review the SAR in conjunction with the Record of Processing Activities (ROPA) to ascertain whether or not personal data is being processed by the school.

The Trust's/School's nominated person will liaise with the relevant information asset owners in order to collate the required information.

Original documents are not required to be provided. A copy can be provided or multiple documents containing personal information can be transposed into a single document.

Any personal information relating to data subjects not named in the SAR must be redacted.

If the request is made electronically, the school should provide the information in a commonly used electronic format. Personal information can also be provided in paper formats.

UK GDPR does not include an exemption for requests that relate to large amounts of data, but the School may be able to consider whether the request is manifestly unfounded or excessive.

Recording of Request

In order to determine if a request can be deemed repetitive, records of SARs will be kept. This record in itself will be subject to any future SARs and should be retained in line with the Trust/School retention schedule.

Compliance

All staff are expected to comply with the School's policies to the highest standards. If any school

employee is found to have breached this policy, they may be subject to the School disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

Definitions

Personal data - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data subject rights – This refers to the rights that the GDPR gives to data subjects in relation to their personal or sensitive data including:

- The right to be informed on what data is processed/shared, how and why
- The right of access (i.e. subject access requests)
- The right to rectification, correcting errors;
- The right to erasure (i.e. the right to be forgotten);
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling using personal data.

Subject Access Request (SAR) – A request made by a data subject for access to personal information the organisation is processing about themselves or on behalf of someone else where they have authorisation or consent from. This can include:

- A description of the personal data;
- Where/how it is being processed;
- The purposes for which it is being processed;
- Details of who is allowed to see the personal data;
- How long it will be kept.

Appendix 2a - Subject Access Request Form

SUBJECT ACCESS REQUEST (SAR) FORM

Article 15 of the UK General Data Protection Regulation (UK GDPR) grants you the right to access your personal data held by The Manor Trust and both Kensington Avenue Primary School and Norbury High School for Girls.

Both schools are part of The Manor Trust, which is the Data Controller for the purposes of data protection law for all personal data processed across both academies.

Please complete this form if you wish to make a request regarding your personal data.

NOTE: This is not a mandatory form – Subject Access Requests made in other formats will also be accepted but this form is designed to help you in providing us with the information we need to deal with your request and speed up the process.

General Information

How long will it take to get my data?
Once we are satisfied that you meet the criteria for disclosure of data under the **UK**

General Data Protection Regulation (UK GDPR) and have provided sufficient information for us to confirm your identity, you should receive a response within one calendar month from that date. However, in certain circumstances, the **UK GDPR** allows us to extend this deadline, depending on the complexity of your request. If we need to extend the response time, we will notify you within one month.

Records may be held in various locations in both paper and electronic formats. If you are only requesting specific information (such as a particular document or electronic data), please specify this clearly, as it may help expedite your request.

Cost
In most cases, we will not charge a fee for complying with a **Subject Access Request (SAR)**. However, if a request is considered manifestly unfounded or excessive, we may charge a "reasonable fee" to cover the administrative costs of fulfilling the request.

Contact information

Title (please tick)

Mr ☐	Miss ☐
Mrs ☐	Other ☐(Specify)
Miss ☐	

Surname:

First name(s):

Date of birth:

Address:

City / County:

Postcode:

Telephone/Mobile (daytime):

Email address:

Relationship to the school:

Employee - Current ☐	Employee - Past ☐
Parent/carer of pupil - Current ☐	Parent/carer of pupil - Past ☐
Supplier - ☐	Other ☐ (specify)

Proof of Identity

We will require proof of your identity before we can respond to your request. In order to prove the applicant's identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card.

List A (photocopy of one from below)		**List B (photocopy of one from below)**	
Identification that clearly shows your name and date of birth.		Documentation that clearly shows your name and current address.	
Passport/Travel Document		A Council Tax bill	
Photo driving licence		Utility bill showing current home address	
Foreign National Identity Card		Bank Statement or Building Society Book	

If you are currently an employee of the Trust or parent/carer to a current pupil at Kensington Avenue Primary or Norbury High School for Girls, you may visit the school office to confirm verification of your identity by an authorised member of staff

We reserve the right to refuse to act on your request if we are unable to identify you.

Information Requested

So that we can locate the data you require efficiently, please complete and answer the following sections to the best of your knowledge.

The Information Commissioner (ICO) has stated that as much information as possible should be provided to assist with tracing a data subject's information.

Please tell us as much as you can about the information you are requesting about.

For example, if you are requesting access to specific information, which might be in regards to your child's attendance or a particular document, this accuracy helps in our search to identify who might have produced it, when and where it may be stored.

Specify period which you request access to the data

From _____ To _____

Declaration

This form must be signed by you (the data subject/parent/carer of the pupil).

I request a copy of the relevant personal data relating to the information provided above. I confirm that the information supplied is correct, and I declare that I am the individual as indicated above.

Please indicate where you believe your personal data is being held:

- The Manor Trust
- Kensington Avenue Primary School
- Norbury High School for Girls
- Both Schools

Warning – a person who unlawfully obtains, or attempts to obtain, personal information is guilty of a criminal offence and is liable to prosecution

Signed: _____ Date: _____

Please send your completed form and proof of identity by email to**:**

DP Lead for The Manor Trust: Markieu Hayden: dplead@themanortrust.org.uk

DP Lead for Norbury High School for Girls: Petra Lindsay: dplead@nhsg.org.uk

DP Lead for Kensington Avenue Primary:: Dean Dumont: dplead@kaps.croydon.sch.uk

Alternatively, you may submit the completed form and proof of identity in person at the relevant school office, or send it by post to the following addresses

Please address to the appropriate school or The Manor Trust as appropriate: The Manor Trust / Norbury High School For Girls / Kensington Avenue Primary School	Kensington Avenue Thornton Heath Surrey CR7 8BT

For office use only

Date SAR received	

Links with other policies

This policy should be read in conjunction with the following related policies and notices:

- Privacy notices
- CCTV Policy
- Subject Access Request (SAR) Procedure
- Freedom of Information (FOI) Policy
- Data breach procedure
- Records management and Retention Policy