DIOCESE OF SOUTHWELL & NOTTINGHAM
MULTI ACADEMY TRUST

DIOCESE OF SOUTHWELL AND NOTTINGHAM MULTI ACADEMY TRUST

DATA PROTECTION POLICY

Approved by the MAT Board of Directors – February 2026

Policy:	Data Protection
Approved by:	SNMAT Board of Directors
Date:	February 2026
Review cycle:	Annual

VERSION CONTROL			
VERSION	**DATE**	**AUTHOR**	**CHANGES**
2020	March 2020	SKP	Page 3 and 9 – additions highlighted Slight amendments (typo's corrected) in the appendices
2022	May 2022	SKP	Page 10 – additional of "Where personal information is requested by the police the academy should request that a Police Disclosure Form is completed (Appendix 7)." Appendix 7 added. Add Cyber Security Policy and IT Technical Guidance to Links to Other Policies.
2023	May 2023	SKP	Page 6 Addition of • Ensuring that a data sharing agreement is in place with any organisation with which the academy intends to share personal data. to responsibilities of Principal/Headteacher Addition of "and staff" to Academy Data Protection Co-ordinator paragraph. Addition of • They have completed the Hays On-line Safeguarding training at least annually; • They have read, understood and follow the academy's Data Protection Policy; under the responsibilities of employees. Page 9 – inclusion of E Safety Policy in list of links to other policies Addition of "Prior to collecting or sharing personal data a Data Protection Impact Assessment (DPIA) template should be completed (Appendix 7) and the DPIA checklist followed." Page 10 amended "SNMAT's equal opportunity policies" to "SNMAT's Equality and Diversity statement".

			Appendix 7 – Inclusion of Data Protection Impact Assessment form Police Data Information Request form becomes Appendix 8.
2024	November 2024		Pg 9 – amendment to wording from E-Safety Policy to E-Safeguarding Policy
2026	January 2026	SKP	Pg 8 – Paras added for Trust IT Manager and Academy IT Manager/Network Manager/Senior IT Engineer responsibilities. Pg 10 - Biometric Data Protection Policy and Artificial Intelligence Guidance & Checklist added to list of other policies this policy links to. Pg 11 Para added to explain amendment to the Data Protection Act that limits the information that has to be provided under a SAR to that which can be identified through a reasonable and proportionate search. Pg 14 – "…if a similar form is not provided by the police themselves." Added. "A legitimate interests assessment (LIA) (Appendix 9) should be completed whenever a request to share data is made by another organisation." Added. "The Trust will follow the ICO Data Sharing Code of Practice." Added. Appendix 7 replaced with ICO model DPIA Appendix 9 Legitimate Interests Assessment Template added.

Contents

Introduction

The Diocese Of Southwell and Nottingham Multi-Academy Trust (SNMAT or The Trust) partner academies collect, store and use certain types of personal information about staff, pupils, parents and other individuals who come into contact with the academy in order provide education and associated functions.

This policy is intended to ensure that personal information is dealt with properly and securely in accordance with the General Data Protection Regulation and other related legislation. It will apply to all personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Scope

This policy aims**:**

- To explain the rationale behind the General Data Protection Regulation;
- To set out roles and responsibilities in relation to the General Data Protection Regulations and Data Protection Legislation;
- To ensure that compliance with the legislation is met;
- To provide guidance for implementation including storing, making secure and providing information.

Rationale

The implementation of the General Data Protection Regulation (GDPR) from 25 May 2018 marks a natural evolution from the 1998 Data Protection Act. The GDPR incorporates most of the same principles of lawful processing but also takes account of new ways of identifying an individual and regulates the use of personal data.

The GDPR provides data subjects with enhanced rights, requires data breaches to be notified to the data subject and the Information Commissioner's Office (ICO), increases the penalties for data breaches and requires data controllers to demonstrate compliance.

General Data Protection Regulation Principles

SNMAT must comply with the General Data Protection Regulation to ensure data is collected and used fairly, stored safely and not disclosed to other persons unlawfully. To do this SNMAT must comply with 6 Data Protection Principles, in summary these state that personal data shall be;

- Processed fairly, lawfully and in a transparent manner;
- Used for specified, explicit and legitimate purposes;
- Used in a way that is adequate, relevant and limited;
- Kept accurate and up to date;
- Kept for no longer than is necessary;
- Processed in a manner that ensures appropriate security of the personal data.

Legal Basis for Collecting and Processing Data

Under the GDPR SNMAT is required to identify the legal basis for collecting and processing personal data. The legal basis can be any of the following:

- Necessary for compliance with a legal obligation;

- Necessary to carry out tasks in the public interest;
- Necessary for the purposes of legitimate interests pursued by the data controller or a third party;
- Necessary to protect the vital interests of a data subject or another person;
- Necessary for the performance of a contract with the data subject;
- Consent has been given for the processing.

Although the majority of data collection and processing activities are carried out under the legal basis of statutory requirements or public task some data processing activities will require consent from the data subject and the regulations for this have been significantly enhanced under GDPR.

Consent must:

- Name the data controller and any third parties that will rely on the consent given;
- Offer a genuine choice and control
- Be freely given, specific and informed
- Be clear and concise about what is being consented to
- Be a positive opt-in
- Be separate from other terms and conditions
- Offer easy ways to withdraw consent
- Be verifiable

Sensitive Personal Data

Sensitive personal data, should be kept to a minimum and as far as possible the information should be kept in an anonymous form. The legislation around sensitive personal data is more strict. Sensitive personal data includes data relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- genetic data;
- Biometric data;
- Health;
- Sex life;
- Sexual orientation.

Breaches of the General Data Protection Regulation

Under the GDPR there is a requirement to report breaches of the General Data Protection Regulation to the Information Commissioner's Office where there is a high risk that an individual may suffer damage by for example:

- Discrimination;
- identity fraud;
- financial loss;
- breach of pseudonymity;
- damage to reputation;
- loss of confidentiality
- any other significant economic or social disadvantage.

Penalties that can be imposed by the ICO in respect of breaches of the GDPR have increased

significantly.

Roles and Responsibilities

Board of Directors - Data Controller

The Diocese of Southwell and Nottingham Multi Academy Trust (SNMAT) is the corporate body registered with the Information Commissioners' Office as a Data Controller and the Directors are ultimately accountable for implementation of the GDPR and must be able to demonstrate compliance with the data protection principles.

Local Governing Bodies

Each of the academies within SNMAT is named on the data protection registration and the Board of Directors has delegated the responsibility for ensuring compliance with the GDPR and the Data Protection policy to the Local Governing Bodies of the academies. The Local Governing Body should appoint a named Governor as having responsibility for Data Protection.

Principal/Headteacher

The Local Governing Body delegates the responsibility for dealing with day to day matters in respect of data protection to the Principal/Headteacher of the academy. He/she is responsible for:

- Implementing any policies developed by SNMAT regarding data protection;
- Determining which members of staff should have access to confidential information;
- Ensuring safe and confidential systems are in place in the academy;
- Providing information to bodies entitled to receive information;
- Providing relevant information about a pupil/student's progress to his/her parents (In this policy statement, "parents" means all those having a parental responsibility for a child);
- Authorising the release of information covered by data protection legislation to outside agencies or external bodies;
- Ensuring that any third party processing data on behalf of the academy is also compliant, that there is a record of the processing activity and that there are appropriate data sharing agreements in place;
- Ensuring that any actual or suspected breach of the General Data Protection Regulations is logged at the academy and reported to the SNMAT Data Protection Officer immediately.
- Ensuring that a data sharing agreement is in place with any organisation with which the academy intends to share personal data.

Data Protection Officer

In accordance with GDPR the SNMAT has appointed a Data Protection Officer (DPO) whose responsibilities include:

- Informing and advising the organisation and its employees about their obligations to comply with GDPR and other data protection laws;
- Monitoring compliance with GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits;

- Being the first point of contact for the ICO and for individuals whose data is processed;
- Ensuring that a risk assessment is carried out in relation to any breach of the GDPR and liaising with the Information Commissioner's Office as necessary;
- Maintaining a register of the legal basis for which data has been processed, who this is shared with and for what reasons;
- Maintaining a log of any breaches of data protection legislation across the Trust.

A separate e-mail contact address, data.protection@snmat.org.uk has been set up to provide a direct point of contact with the Data Protection Officer.

Academy Data Protection Co-ordinator

Each academy is required to appoint an Academy Data Protection Co-ordinator (ADPC) who is responsible for:

- acting as the main point of contact between the academy and the DPO in the case of a data breach or Subject Access Request (SAR);
- leading on the response to any SARs in respect of pupils and staff at the academy.

Trust IT Manager

The Trust IT Manager is responsible for:

- Overseeing technical and organisational security measures to ensure the Trust and partner academies meets its obligations and prevents unauthorised access, loss, destruction or damage to data.
- Assisting the Data Controller, Data Protection Officer, Academy Data Protection Coordinators and Academy IT Support Teams by providing technical assistance for DPIAs, risk assessments, responding to Data Breaches and Data Subject Rights (including SARs).

Academy IT Manager/Network Manager/Senior IT Engineer

The Academy IT Manager/Network Manager or Senior IT Engineer is responsible for:

- Implementing technical and organisational security measures to ensure the organisation meets its obligations and prevents unauthorised access, loss, destruction or damage to data.
- Assisting the ADPC by providing technical assistance for DPIAs, risk assessments, responding to Data Breaches and Data Subject Rights (including SARs).

Staff

The academy should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users are assigned a clearance that will determine which files are accessible to them. Access to protected data should be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

In respect of their own personal data employees are responsible for:

- Ensuring any information they provide to SNMAT in connection with their employment is accurate and up to date;
- Informing SNMAT of any changes to information they have previously provided e.g.

changes of address;
- Checking the information that the academy or SNMAT send out from time to time giving details of information held and processed;
- Informing the academy or SNMAT of any errors or changes.

All employees are responsible for ensuring that:
- Any personal data to which they have authorised access is kept secure;
- They have completed the Hays On-line Safeguarding training at least annually;
- They have read, understood and follow the academy's Data Protection Policy;
- They have read, understood and follow the academy's Bring Your Own Device (BYOD) Policy where appropriate;
- Personal information is not disclosed either orally or in writing deliberately, accidentally or otherwise to any unauthorised third party – particular care must be taken when using e-mail or faxing confidential data;
- No personal information is given to a third party over the telephone. All requests should be confirmed in writing and replied to in writing;
- Any actual or suspected breach of the General Data Protection Regulations is to be reported to the Academy IT Support Team, ADPC and Principal/Headteacher immediately.

Penalties for breaches of data protection legislation have increased significantly under GDPR and disciplinary action will be taken against any employee who breaches any of the instructions or procedures following from the Data Protection Policy.

Objectives

SNMAT is committed to maintaining the principles of the GDPR and ensuring that its academies comply with the requirements of this and other associated legislation. All academies will:

- Inform all individuals and, where appropriate, their parent or guardian as to the purpose of collecting any information from them, as and when they ask for it by means of a privacy notice;
- Be clear which legal basis is used to collect and process specific personal data and ensure that the SNMAT register is kept up to date by notifying the Data Protection Officer;
- Check the quality and accuracy of the information held and regularly review the records to ensure information is not held longer than is necessary (see Records Management Policy and Records Management Toolkit);
- Ensure that when information is authorised for disposal it is done appropriately, using a confidential information disposal service if necessary, and logged;
- Ensure appropriate security measures are in place to safeguard personal information whether held in paper files or on a computer system;
- Share personal information with others only when it is necessary and legally appropriate to do so, ensuring that pupil names are replaced with unique pupil numbers in the records before the data is transferred where possible;
- Follow clear procedures for responding to requests for access to personal information known as subject access in the DPA and 'the right of access by the data subject' under the GDPR including the right to be forgotten;
- Ensure a clear policy and procedures for the automatic backing up, accessing and restoring all data held on academy systems is in place, including off-site backups;

- Ensure controls put in place by remote/cloud based data services providers to protect the data are satisfactory.
- maintain a register of the legal basis for which data has been processed, with whom this is shared and for what reasons;
- maintain a log of any breaches of data protection legislation.

Links with Other Policies

The Data Protection Policy must be read in conjunction with the other following policies and procedures:

Data Breach Notification Procedure
Procedure for Receiving and Responding to a Subject Access Request
Bring Your Own Device (BYOD) Policy
ICT Policy and Technical Guidance
Cyber Security Policy
Social Media Policy
E-Safeguarding Policy
Records Management Policy
Freedom of Information Policy
Biometric Data Protection Policy
Artificial Intelligence Guidance & Checklist

Guidance for Implementation

Prior to collecting or sharing personal data a Data Protection Impact Assessment (DPIA) template should be completed (Appendix 7) and the DPIA checklist followed.

Legal Basis for Collecting and Processing Data

Data held about pupils/students must be collected and processed for specific purposes required by law, such as completing returns to the DfE. Pupil/student information is also collected and retained locally because it is necessary to the purpose of educating children and young people, for example tracking pupil achievement and assessing special educational needs. The collection, processing and sharing of medical information may be vital to their interests. In some cases, pupil information may be shared with service providers where contracts are put in place to benefit pupils/parents e.g. communication with parent services or payment for school meals services. Consent must be obtained where data is collected which is not required for legal purposes or in order to carry out the task of educating pupils. Wherever possible SNMAT academies should look for an alternative legal basis for processing data but there will be some cases where obtaining consent will be unavoidable, for example the use of photographs for publicity functions.

Information about staff is also collected and processed in order to perform key tasks e.g. recruitment, performance monitoring, recording absence and health and safety matters.

Academies must ensure they have data sharing agreements in place with any organisation with whom they share data. The Data Protection Officer must be informed of any new data sharing agreements to ensure the register is kept up to date.

Sensitive Personal Data

Sensitive personal data is periodically required by the government for the purposes of equal opportunity monitoring and as such would be covered under the legal basis of statutory requirement. In implementing this policy the academy Principal/Head teacher and all members of staff must consider SNMAT's Equality and Diversity statement. The academy must ensure that no student or member of staff is disadvantaged on the grounds of gender, race, disability, sexual orientation, age, religion or belief.

The Trust recognises that biometric data, including facial recognition, fingerprints, or any technology that analyses unique physical characteristics, constitutes special category personal data and must only be collected and processed in strictly limited circumstances. In line with the concerns raised by the Information Commissioner's Office (ICO) in its correspondence to North Ayrshire Council regarding the use of Facial Recognition Technology in schools, the Trust will not deploy biometric systems unless a compelling, proportionate, and clearly evidenced justification exists, and only where less intrusive alternatives cannot reasonably achieve the same purpose. Any proposed use of biometric data must undergo a full Data Protection Impact Assessment (DPIA), include consultation with affected individuals, and rely on explicit, freely given consent, with genuine alternatives offered without detriment. Biometric data will never be used for routine convenience, and no pupil, parent, or staff member will be pressured to provide it. Where biometric processing is approved, the Trust will ensure strict security controls, minimal data retention, and ongoing review of necessity and proportionality (see Biometric Data Processing Policy).

Rights of Subject Access (SAR)

All individuals have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data and other supplementary information so that they are aware of and can verify the lawfulness of the processing;

On receipt of a SAR the Trust will conduct a reasonable and proportionate search for personal data as per Section 15(1A) of the UK GDPR, as amended by Section 78 of the Data (Use and Access) Act 2025 (DUA Act) on systems and formats for which it is the data controller. This amendment to the Data Protection Act confirms that organisations are not expected to conduct exhaustive searches, especially where the effort involved would be disproportionate to the value of the data retrieved. In practice "reasonable" means searching systems and locations where personal data is likely to be held using appropriate keyword and filters to locate relevant data. The organisation is not required to search inaccessible or irrelevant systems such as backups and archives unless retrieval is straightforward. Where searches result in large datasets or fragmented records where the likelihood of finding relevant data is low a request may be made for more specific search criteria to reduce the volume and complexity of the data.

There is no charge for a SAR in most cases. However, a reasonable fee based on the administrative cost of providing the information, may be charged for additional requests for the same material, voluminous or excessive requests. The academy must respond without undue delay and at least within 1 month, although additional time will be available for complex requests.

This also applies to requests for:

- rectification of inaccurate data;

- erasure;
- restriction of processing
- data portability;
- objections to automated processing

In the event of a SAR please refer to the Procedure for Receiving and Responding to Subject Access Requests for further information.

Data Security

The Integrity and Confidentiality Principle requires that personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. In order to ensure compliance with this principle academies must ensure that only authorised staff can process the personal data.

This should include the following physical security measures:

- Personal information must be kept in a locked filing cabinet with restricted access or stored in a secure folder with restricted access on the academy's computer network;
- Positioning of PC screens in classroom/offices for maximum security;
- Restricting access to the academy office;
- Restricted access to server and infrastructure hardware;
- Restricting access to the School Information Management System;
- Implementing a clear desk policy;
- Using secure, tracked and signed for postage for confidential data;
- Ensuring printing can only be accessed securely;
- Ensuring that confidential data and computers are disposed of securely;

The following Technical Security Measures should be in place in each academy:

- a strong password policy for data assets held on computer;
- a policy of password changes if the user believes it has been compromised;
- cancellation of access when staff leave;
- Academy managed social media accounts should comply with the MAT Social media policy guidelines;
- up to date anti-virus, anti-malware and local machine firewall enable and appropriately configured;
- up-to-date security patches applied to all computers;
- appropriately configured edge firewall;
- appropriate user web filtering;
- encryption on all devices that leave school premises;
- use of authorised cloud storage and access portals wherever possible to minimise the need to store data on portable devices.
- Implementation of a BYOD policy;
- Appropriate secured wi-fi connectivity;

Data Sharing

Use of Personal information within the Academy

There will be a need for relevant employed staff, contracted staff or volunteers working within the academy to be informed of individual student information both for academic and pastoral reasons.

Academic data will be available for all teaching and support staff to enable them to plan and set targets effectively. Teaching staff will discuss individual achievement data with the individual concerned and their parents. However, the unnecessary publication of individual achievement data with groups of students should be avoided.

Some members of staff will need to have an overview both of achievement data and personal information data and should discuss progress with the individual student and parents, as appropriate. They should also inform relevant teaching and support staff of individual personal data if it is deemed necessary to ensure that the student is taught and catered for appropriately.

Personal information regarding individual students must not be discussed with members of the public by anyone working in the academy.

All teaching and support staff should be notified of any medical information relating to students at the start of each academic year or on admission during the year.

Staff must bear in mind that information retained by them in locally held records and/or mark books is not confidential. Students and their parents are entitled to know what is kept on file about the student (and/or about the parent(s)).

Employees should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual employee.

Provision of Information to External Organisations

Information relating to students' academic achievements and progress must be published annually to the DfE, in line with current DfE requirements. Any other academic data relating to past or present students used for any purpose outside of the academy must be presented in an anonymous format.

Sensitive personal information about past or present students must only be disclosed to external agencies acting for and on behalf of individual students or their parents. This may include some of the following agencies and professionals:

- Social Services
- Educational psychologists
- Medical professionals
- Education Support Services
- Police
- Youth Inclusion Team

Parental permission must normally be sought prior to involving outside agencies. Exceptions to this rule will include matters relating to Child Protection (which should only be referred through the academy's Designated Safeguarding Lead (DSL)) and information relating to criminal activity.

Medical information and matters concerning child protection must be kept in a confidential file and will be supplied to relevant authorities where the Principal/Headteacher deems it appropriate (e.g. police or social services). Only the Principal/Headteacher and staff authorised by the Principal/Headteacher may have access to this file. Where personal

information is requested by the police the academy should request that a Police Disclosure Form is completed (Appendix 8) if a similar form is not provided by the police themselves.

Medical emergency procedures will take account of prior information collected from medical forms completed by parents. In cases of medical emergency, parents must be notified of any action taken without delay.

Under no circumstance must personal information about a student be passed on to representatives of the Media. No information about students will be provided to marketing companies, unless the parent of the student concerned has given specific written permission.

The academy must be clear about the legal basis for sharing the personal information and must maintain a register showing the data it shares, with whom and for what reason. The academy must also be assured that the external organisation with whom it is sharing the data also complies with the GDPR. A legitimate interests assessment (LIA) (Appendix 9) should be completed whenever a request to share data is made by another organisation.

The Trust will follow the ICO Data Sharing Code of Practice.

General Requests for Information

Personal data must be treated as confidential and disclosures of data must be in accordance with the provisions of the GDPR and the SNMAT policies and procedures.

All requests for information about students must go to the Principal/Headteacher, who will determine whether it is lawful and appropriate to release the information. Members of staff who receive personal requests for references or other information about current or past students must inform the Principal/Headteacher before providing the information to ensure that they are acting within the law and official guidance. Any concerns regarding requests for information should be referred to the SNMAT Data Protection Officer.

Monitoring the Use of Electronic Communications

As the Data Controller the Trust is legally responsible for any processing of its data. Therefore, while the Trust/academy aims not to intrude into the private lives of staff or students, it reserves the right to monitor the use of academy computers, video and audio machines, phones and fax machines, social media posts, e-mail conversations or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems to ensure its policies and procedures in relation to data protection are being complied with. Staff consent to such monitoring by acknowledgement of this policy and their use of such resources and systems. Appropriate records of any monitoring will be kept, which can be accessed on request to the Principal/Headteacher (or the senior member of staff authorised by the Principal/Headteacher).

Breaches of the General Data Protection Regulation

Under the GDPR there is a requirement to report breaches of the General Data Protection Regulation to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Any actual or suspected breach of the General Data Protection Regulations must be reported to the SNMAT Data Protection Officer immediately. The Data Protection Officer will carry out a Risk Assessment in relation to the

breach and will liaise with the Information Commissioner's Office.

The academy must keep a log of any breaches of the general data protection regulations and the Data Protection Officer will keep a record of all breaches across SNMAT. The breach log for the academy will be reviewed regularly by the Local Governing Body and the Board of Directors will review breaches across the MAT.

In the event of a data breach please refer to the Data Breach Procedure.

Penalties for breaches of data protection legislation have increased significantly under GDPR and disciplinary action will be taken against any employee who breaches any of the instructions or procedures following from the Data Protection Policy.

Review

This policy is reviewed annually by the Trust in consultation with the recognised trade unions. The application and outcomes of this policy will be monitored to ensure it is working effectively.

Appendix 1

Key Retention Periods for Personal Data

Guidance regarding the retention periods for all documentation relating to schools/academies is available in the Records Management Toolkit for Schools, produced by the Information and Records Management Society. Secure disposal is required for all the following records:

Pupils/Students

Description	Retention Period
Child Protection	Date of Birth + 25 years
Admission Registers	Last entry + 7 years
Attendance Registers	Date of register + 3 years
Pupil Files - Primary	While the pupil remains at the school
Pupil files - Secondary	Date of Birth + 25 years
SEN files, reviews and IEPs	Date of Birth + 25 years
Internal Exam Results	Current Year + 5 years
Statement of SEN	Date of Birth + 30 years
Advice and information to Parents re SEN	Closure + 12 years
Accessibility Strategy	Closure + 12 years
Parental Permission Slips for Trip where there has been no major incident	Conclusion of trip
Parental Permission Slips for Trip where there has been a major incident	Date of Birth of pupil concerned + 25 years
Walking Bus registers	Date of register + 3 years
Exam and SATS Results	Current Year + 6 years
Free School Meal Registers	Current Year + 6 years

Academy Workforce

Personal information should not be retained on the employment record for any longer than is necessary for the purpose required but equally it should not be discarded if doing so renders the record inadequate.

Description	Retention Period
Timesheets, sick pay	Current year + 6 years
Staff Personal files	Termination + 7 years
Interview notes and recruitment records	Date of interview + 6 months
Disciplinary Proceedings Oral warning Written warning level 1 Written warning level 2 Final written warning Case not found	 Date of warning + 6 months Date of warning + 6 months Date of warning + 12 months Date of warning + 18 months Immediately on conclusion of case unless child protection related

Accident or injury at work	Date of incident + 12 years
Maternity pay records	Current year + 3 years
Retirement Benefits Schemes Records	Current year + 6 years

These timescales can be extended where there is a **justified business reason** for doing so not merely that it might be useful to hold such documentation.

Small quantities of confidential waste may be disposed of on site using an office shredder, which should be located in a secure area. Where larger quantities of confidential information need to be disposed of, a company specialising in the disposal of confidential waste should be used. Under no circumstances should confidential records be placed in rubbish bins or skips.

The person responsible for records management in the Academy is:	Sue Onley
The person responsible for disposing of confidential information within the required deadlines is:	Sue Onley

Appendix 2 a

Privacy Notice (How we use pupil information)

Why do we collect and use pupil information?

We collect and use pupil information under the lawful basis of legal obligation and public task. Examples of data collection for legal obligation purposes are the Department for Education Censuses required under the Education Act 1996 – this information can be found in the census guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools

To assist with the performance of official functions the academy also retains data locally for pupil achievement tracking.

We also collect and use pupil information where it is vital to their interests eg medical information and where consent has been obtained, for example for a photograph to be included in publicity material.

In some cases pupil information may be shared with service providers where contracts are put in place to benefit pupils/parents eg communication with parent services or payment for school meals services

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard pupil health and wellbeing
- to be included in publicity materials or on the website
- to assist with the collection of payment for pupil meals
- to assist with communication

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as examination registration number)
- Relevant medical information (name and address of doctor, allergies, medical conditions)
- Special educational needs information
- Exclusions/behavioural information
- Post 16 learning information

Collecting pupil information
Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data
In Primary academies, we hold pupil data until the pupil transfers to secondary school when the pupil records transfer with them. In secondary academies, we hold pupil data until they reach the age of 25 years. Records are retained in accordance with the guidance in the Records Management Toolkit for Schools produced by the Information and Records Management Society.

Who do we share pupil information with?
We routinely share pupil information with:

- Schools/academies/multi academy trusts that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- service providers of management information and assessment tracking software
- service providers of parent communication services
- service providers of vouchers for provision of services such as breakfast clubs

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services
What is different about pupils aged 13+?
Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Our pupils aged 16+
We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and

retention and use of the data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Headteacher of the academy or the SNMAT Data Protection Officer at data.protection@snmat.org.uk.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

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

Headteacher of academy
Academy address
Academy phone number

Or

Data Protection Officer
data.protection@snmat.org.uk

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Appendix 2b

Workforce Privacy Notice

Policy Statement

During an individual's time with the Diocese of Southwell of Nottingham Multi Academy Trust, we will use information that we gather in relation to them for various purposes. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from the individual directly and data about the individual that we obtain from other people and organisations. We might also need to continue to hold an individual's personal data for a period of time after they have left the school. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about our workforce, why we process that data, who we share this information with, and the rights of individuals in relation to their personal data processed by us.

What information do we process in relation to our workforce?

We will collect, hold, share or otherwise use the following information about our workforce:

- personal information (such as name, address, home and mobile numbers, personal email address, employee or teacher number, national insurance number, and emergency contact details)

- contract information (such as start dates, hours worked, post, roles and salary information, bank/building society details)

- work absence information (such as number of absences and reasons (including information regarding physical and/or mental health), holiday records)

- qualifications/training courses attended and, where relevant, subjects taught (such as training record)

- performance information (such as appraisals and performance reviews, performance measures including performance management/improvement plans, disciplinary or grievance records)

- other information (such as pension arrangements (and all information included in these necessary to administer them), time and attendance records, information in applications made for other posts within the school, criminal records information (including the results of Disclosure and Barring Service (DBS) checks), details in references the school receives or provides to other organisations, CCTV footage and images)

We will also use special categories of data including gender, age, ethnic group, sex or sexual orientation, religious or similar beliefs, political opinions, trade union membership, information about health, genetic information and biometric data. These types of personal data are subject to additional requirements.

Where do we get information from about our workforce?

A lot of the information we have about our workforce comes from the individuals themselves. However, we may also obtain information from tax and regulatory authorities such as HMRC, previous employers, your trade union, the DBS, our insurance benefit administrators, consultants and other professionals we may engage, recruitment or vetting agencies, other members of staff, students or their parents, and publicly available resources including online sources. In addition we may obtain information from automated monitoring of our websites and other technical systems such as our computer networks and systems, CCTV and access control systems, communications systems, remote access systems, email and instant messaging systems, intranet and internet facilities, telephones, voicemail and mobile phone records.

Why do we use this information?

We will process the personal data of our workforce for the following reasons:

1. Where we are required by law, including:

    - To comply with the law regarding data sharing (see further below)
    - To comply with specific employment law requirements, including our obligations as an employer under employment protection and health and safety legislation, and under statutory codes of practice such as those issued by ACAS
    - To comply with legal requirements in relation to equalities and non-discrimination

2. Where we are required by any contract with our workforce, such as employment contracts, including:

    - To make payments to our workforce, such as salary payments
    - To deduct tax and National Insurance contributions
    - To make a decision about recruitment
    - To check individuals are legally entitled to work in the UK
    - Administering employment contracts
    - Conducting performance and/or attendance reviews
    - Making decisions about salary and compensation
    - Liaising with pension providers
    - Providing benefits
    - To administer and pay trade union premiums and register the status of a protected employee

3. Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest, including:

    - To enable the development of a comprehensive picture of the workforce and how it is deployed
    - To inform the development of recruitment and retention policies
    - To safeguard our pupils and other individuals
    - To ensure safe working practices
    - In the interests of ensuring equal opportunities and treatment

4. Where we otherwise have the consent of the individual

Whilst the majority of processing of personal data of our workforce will not require consent, we will inform individuals if their consent is required and seek that consent before any processing takes place. In the limited circumstances where individuals have provided their consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw their consent for that specific processing at any time. To withdraw their consent, they should contact Sarah Perry – Data Protection Officer SNMAT.

Why do we use special category personal data?

We may process special category personal data of our workforce for the following reasons:

1. To carry out our legal obligations in relation to employment law, where this is in accordance with our Data Protection Policy

2. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy.

3. For the purposes of preventative or occupational medicine in order to assess an individual's working capacity and/ or the need for reasonable adjustments.

4. Where we otherwise have an individual's explicit written consent – subject to the restriction set out above on the use of consent in an employment relationship.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

Failure to provide this information

If our workforce fails to provide information to us then this may result in us being unable to perform the employment contract, or we may be prevented from complying with our legal obligations.

How long will we hold information in relation to our workforce?

We will hold information relating to our workforce only for as long as necessary. How long we need to hold on to any information will depend on the type of information. For further detail please see our Records Management Policy.

Who will we share information with about our workforce?

We routinely share information about our workforce with:

- The Department for Education[and/or the ESFA], in compliance with legal obligations of the school to provide information about our workforce as part of statutory data collections
- Contractors, such as payroll providers, to enable them to provide an effective service to the school and government agencies such as HMRC and DWP regarding tax payments and benefits
- Our professional advisors including legal and HR consultants

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data.

Contact details for the Department can be found at https://www.gov.uk/contact-dfe.

Rights of our workforce in relation to their personal data

All of our workforce have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact:

Trust HR Officer
payroll@snmat.org.uk

Please also refer to our Data Protection Policy for further details on making requests for access to workforce information.

Individuals also have the right, in certain circumstances, to:

- Object to the processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Restrict processing of their personal data
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wishes to exercise any of these rights then they should contact the Trust's HR Officer. The law does not oblige the Trust/Academy to comply with all requests. If the Trust/Academy does not intend to comply with the request, then the individual will be notified of the reasons why in writing.

Concerns

If an individual has any concerns about how we are using their personal data then we ask that they contact our Data Protection Officer in the first instance. However an individual can contact the Information Commissioner's Office should they consider this to be necessary, at https://ico.org.uk/concerns/.

Contact

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

Data Protection Officer
data.protection@snmat.org.uk

Data Collection Form *(Name of Academy)*

Date **.....**

Surname			Forename		
Middle Name			Chosen Name		
Date of Birth					
Address:					
Postcode:			Tel.No.:(Landline)		
Parent/Carer Name:		Occupation:		Mobile: (to receive texts)	
Address if Different from Above					
Email:					
Parent/Carer Name:		Occupation:		Mobile:	
Address if Different from Above					
Email:					

Please note that parent/carer contact details may be shared with companies providing services to the academy for the benefit of parents, such as text messaging

Emergency Contacts other than Parent/Carers named above:				
	Phone Number:		Relationship:	
	Phone Number:		Relationship:	

Please list below the names of authorised adults who may be collecting your child(ren) throughout the year:		

Ethnic Origin: (please tick the correct description)					
AIND – Indian		APK – Pakistani		BCRB – Black / Caribbean	
CHNE – Chinese		MBA – White / Black African		WHT – Traveller	
MWAS – White / Asian		MWB – White / Black Caribbean		WIRI – Irish	
MOT – Any other mixed background		WBRI – White British		WOTH – Any other white background	

My child's first language is:		Religion:		Home Language:	
Any Family Links in School:					

Member of HM Forces	**YES**		**NO**	

Permission to sit in front of mini-bus	**YES**		**NO**	

Meals:	1.Free school meal entitlement		2.Paid School Dinners		3.Sandwiches	4.Home	
Special Dietary Requirements			Vegetarian		Halal		

(If your child has sandwiches but is entitled to free school meals, please tick number 1)

Medical Information

Doctor's Name:		Surgery:	
Special medical factors/allergies:			

Asthmatic:	YES		NO		Inhaler provided:	YES		NO	

Any children requiring inhalers must have an inhaler to keep in school and up-to-date medication at all times.
Parents must ensure they complete an asthma card detailing the condition and the amount of medication required.

I understand that for the safety of my child, I should telephone school as soon as possible on the first day of absence.

Please note that this information will remain on file until your child leaves unless the academy is notified that anything has changed. It is important to contact the academy with any changes throughout the year, especially changes to emergency contact numbers, mobile phones, allergies or asthma etc. An information update request may be made annually to ensure that this remains as up to date as possible.

General Data Protection Regulation

The Diocese of Southwell and Nottingham Multi Academy Trust is registered to collect and process personal information with the Information Commissioner's Office. The academy needs to collect this information because it is legally required to do so and because it needs the information in order to do its job. It is legally required to share some of the data with the Local Authority and the DfE. Contact details for parents may be shared with companies which provide services for the academy for the benefit of parents. Medical details are collected for the protection of your child. The academy has a duty to protect this information and to keep it up to date. Full details may be found in the attached privacy notice.

Signed:_____ (Parent / Carer) Date: _____

Appendix 4a

DIOCESE OF SOUTHWELL & NOTTINGHAM MULTI ACADEMY TRUST

CONFIDENTIAL PARENTAL CONSENT FORM

Local Visits

Full name of Child/Student in block capitals _____

We/I give my consent for my child to participate in the following visits in the local area:

Walks to church	YES/NO	
Walks around the village	YES/NO	
Sports events at local schools	YES/NO	
Swimming	YES/NO	
Visits to museums	YES/NO	
	YES/NO	
	YES/NO	
	YES/NO	

Parents will be informed of local visits and asked to complete an acknowledgement slip as appropriate.

Please note that you have the right to withdraw your consent at any time by contacting the academy either by e-mail to …… or telephone …… or by contacting the Data Protection Officer at data.protection@snmat.org.uk

Consent forms for day trips and residential visits will also need to be completed as required.

Appendix 4b

DIOCESE OF SOUTHWELL & NOTTINGHAM MULTI ACADEMY TRUST

CONFIDENTIAL PARENTAL CONSENT FORM

Medical Information for Visits

Please note that the information on this form will be held by the member of staff in charge when a day visit takes place. This information is being collected and processed in the vital interests of your child.

Full name of Child/Student in block capitals _____

Please give details of any medication your child requires:

Name of Medication	Dosage	Times of day or circumstances to be given	Method of administration

I give my consent for a member of staff to administer the above medication, which I will deliver to the group leader before the visit. I understand the staff leading the visit are not qualified medical practitioners but that they will take reasonable care in the administration of the medication and will endeavour to respond appropriately should emergency treatment be required.	YES/NO	
I give my consent for my son/daughter to self-administer the above drugs.	YES/NO	
Is your son/daughter allergic to any medication?	YES/NO	
If YES please specify		
When did your son/daughter last receive a tetanus injection?	Date	
Does your child have any special dietary requirements?	YES/NO	
If YES please specify		

Do you agree to your son/daughter receiving emergency medical treatment as considered necessary by the medical authorities present	YES/NO	
• anaesthetic	YES/NO	
• blood transfusion	YES/NO	

Please note that this consent will remain in force until your child has left the school unless you rescind it. You have the right to withdraw your consent at any time by contacting the academy either by e-mail to …… or telephone …… or by contacting the Data Protection Officer at data.protection@snmat.org.uk

Signed _____ Parent/Guardian

Appendix 4c

DIOCESE OF SOUTHWELL & NOTTINGHAM
MULTI ACADEMY TRUST

CONFIDENTIAL PARENTAL CONSENT FORM

Photograph and Media Permission

Full name of Child/Student in block capitals _____

The use of digital/video images plays an important part in learning activities. Pupils/students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Photographs (printed and digital) and/or video recordings of school activities used for internal records, records of achievement, evidence of learning opportunities and assessment are legally permissible as part of the academy's purpose.

However, your permission is required for the academy to use photographs and/or videos for marketing, promotion, fundraising and school communications purposes in accordance with the SNMAT Data Protection Policy. We will ensure that when images are published that the young people cannot be identified by the use of their names.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children for the following reasons:

Displays in and around the school and Trust (eg on noticeboards, banners etc)	YES/NO	
Academy and Trust publications, printed or digital *(Eg prospectus, newsletters, school magazines)*	YES/NO	
Academy and Trust websites	YES/NO	
Academy and Trust social media (eg class blogs, facebook page, twitter feed)	YES/NO	
Local and National news publications	YES/NO	
Local and National television networks	YES/NO	
Other *(must be specified)*	YES/NO	

Parent / Carers Name:

Signed: .....

Date: .....

Please note that this consent will remain in force until your child has left the school unless you rescind it. You have the right to withdraw your consent at any time by contacting the academy either by e-mail to …… or telephone …… or by contacting the Data Protection Officer at data.protection@snmat.org.uk

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/ made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils/students in the digital/video images.

I agree that if I take digital or video images at, or of, academy events, which include images of children other than my own, I will abide by these guidelines in my use of these images.

Signed: ……

Date: ……

Appendix 4d

DIOCESE OF SOUTHWELL & NOTTINGHAM MULTI ACADEMY TRUST

CONFIDENTIAL PARENTAL CONSENT FORM

Use of Biometric Systems Permission Form

*If the academy uses biometric systems (e.g. fingerprint / palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc. it must (under the GDPR legislation) seek permission from **both** parents or carers.*

The academy uses biometric systems for the recognition of individual children/students in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The academy has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in an academy context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a pupil's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above student / pupil, I agree to the school using biometric recognition systems, as described above. I understand that the images cannot be used to create a whole fingerprint / palm print of my child and that these images will not be shared with anyone outside the school.	Yes / No

Signed: .....

Date: .....

Please note that this consent will remain in force until your child has left the school unless you rescind it. You have the right to withdraw your consent at any time by contacting the

academy either by e-mail to …… or telephone …… or by contacting the Data Protection Officer at data.protection@snmat.org.uk

Appendix 5

ICO Breach Notification Report

1. Organisation Details

Name of Trust	
Data controller's registration number (if applicable)	
Data Protection Officer	
Contact Details	

2. Details of the data protection breach

Set out the details of the breach and ensure that all mandatory (*) fields are completed.

(a)	* Please describe the incident in as much detail as possible.
(b)	* When did the incident happen?
(c)	* How did the incident happen?
(d)	If there has been a delay in reporting the incident to the ICO please explain your reasons for this.
(e)	What measures did the organisation have in place to prevent an incident of this nature occurring?

(f)	Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. Details of the Personal Data placed at risk

Set out the details of the personal data placed at risk as a result of the breach and ensure that all mandatory (*) fields are completed.

(a)	* What personal data has been placed at risk? Please specify if any financial or special category (sensitive) personal data has been affected and provide details of the extent.
(b)	* How many individuals have been affected?
(c)	* Are the affected individuals aware that the incident has occurred?
(d)	* What are the potential consequences and adverse effects on those individuals?
(e)	Have any affected individuals complained to the Academy/Trust about the incident?

4. Containment and recovery

Set out the details of any steps the Academy/Trust has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) * Has the [Trust/Academy/School] taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

(b) * Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

(c) What steps has the [Trust/Academy/School] taken to prevent a recurrence of this incident?

5. Training and guidance

Set out the details of any steps the Trust has taken to contain the breach and/or to recover the personal data and ensure that all mandatory (*) fields are completed.

(a) As the data controller, does the [Trust/Academy/School] provide its staff with training on the requirements of Data Protection Legislation? If so, please provide any extracts relevant to this incident here.

(b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

(c) As the data controller, does the [Trust/Academy/School] provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

(a) * Have you reported any previous incidents to the ICO in the last two years?

YES / NO

(b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

(a)	Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
(b)	Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.
(c)	Have you informed any other regulatory bodies about this incident? If so, please provide details.
(d)	Has there been any media coverage of the incident? If so, please provide details of this.

This form was completed on behalf of Trust by:

Name: ……

Role: ……

Date and Time: ……

Appendix 6

Risk Assessment Record

Activities covered by this assessment:	**BREACH OF PRIVACY**		
Site Address/Location:			

Compliance with DPA/GDPR Risk Step 1	Who might be harmed and how *Step 2*	Existing Control Measures: *Step 3*	Risk Rating			Further action Step 3 Consider hierarchy of controls	Actions Step 4			Risk Rating		
			Likelihood	Severity	Risk Rating		Who (Name)	When (Date)	Complete (Date)	Likelihood	Severity	Risk Rating
Consider if any additional hazards are created and control measures are required if this activity is undertaken in non-routine or emergency conditions							Review Date :					
Assessors Signature:		Date:			Authorised By:				Date:			

Potential Severity of Harm				
	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low **(The event is unlikely to happen)**	Medium **(It is fairly likely it will happen)**	High **(It is likely to happen)**
		Likelihood of Harm Occurring		

Risk Definitions	
Low	Controls are adequate, no further action required, but ensure controls are monitored and any changes reassessed.
Medium	Consideration should be given as to whether the risks can be reduced using the hierarchy of control measures. Risk reduction measures should be implemented within a defined time periods. Arrangements should be made to ensure that the controls are maintained and monitored for adequacy.
High	Substantial improvements should be made to reduce the level to an acceptable level. Risk reduction measures should be implemented urgently with a defined period. Consider suspending or restricting the activity, or applying interim risks controls. Activities in this category **must** have a written method statement/safe system of work and arrangements must be made to ensure that the controls are maintained and monitored for adequacy.

Appendix 7

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 8

Disclosure Request

Schedule 2 Part 1 Paragraph 2 Data Protection Act 2018

1. Requestor

Name:	
Job title:	
Organisation:	
Address:	
Email:	
Tel:	

2. Data subject

Name:	
Address:	
Other relevant identifying information:	

3. State the specific information you require

4. With reference to Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018,

state why you require this information.

5. **State what you intend to do with the information and for how long you will retain it.**

6. **State how not providing the information requested would prejudice the stated purpose set out in 4. and 5. above.**

7. **If you are of the opinion that to inform the individual that we have shared this information with you would prejudice your stated purpose, please state why.**

8. **Information provision**

If we hold information how would you like the information to be provided?

☐ Electronically via secure email

☐ Collection in person

We will notify you if we do not hold information or your request for disclosure is refused

9. **Declaration and authorisation**

The authorising officer must be of the rank of Inspector or higher. If an Inspector is not

available, we will accept an email from an Inspector attaching this form and confirming their approval.

Declaration:

I certify that:

- Information requested is compatible with the stated purpose (section 4) and will not be used in any way incompatible with that purpose
- I understand information given on this form is correct
- I understand that if any information given on this form is incorrect, I may be committing an offence under Section 170 Data Protection Act 2018

Requestor:

Signed:	
Dated:	

Authorising Officer:

Name:	
Job title:	
Signed:	
Dated:	

Where to send your request

Send this form to:

Email:

[Insert email address]

Postal address:

[Insert contact details]

APPENDIX 9

LEGITIMATE INTERESTS ASSESSMENT TEMPLATE

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?
Reasonable expectations
• Do you have an existing relationship with the individual? • What's the nature of the relationship and how have you used data in the past? • Did you collect the data directly from the individual? What did you tell them at the time? • If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? • How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? • Is your intended purpose and method widely understood? • Are you intending to do anything new or innovative? • Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation? • Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact
• What are the possible impacts of the processing on people? • Will individuals lose any control over the use of their personal data? • What is the likelihood and severity of any potential impact? • Are some people likely to object to the processing or find it intrusive? • Would you be happy to explain the processing to individuals? • Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	

LIA completed by	
Date	

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.