MacIntyre Academies

Data Protection Policy

Version 10

V.	Purpose/ Change	Responsibility	Date
For previous changes see end of policy			
V10	Section 2: Added a reference to the MAT Artificial Intelligence (AI) Policy, removed reference to MAT Remote Surveillance Policy, which is not in use. Section 3: New section- Definition Section 4: Re-written - Responsibilities Section 15.3: Clarified that a SAR can be made verbally or in writing. Added that where an exemption is used, it will be recorded as well as the justification. This will be provided to the requestor when appropriate to do so. Section 15.4: Clarified that if a child's competency is brought into question, the Executive Leader for Education and Care Section 15.5: Addition that the Trust is not legally obliged to respond to educational record requests in the same way as a maintained school. Section 15.8: The right to restrict processing, new paragraph with more detail Section 15.9: The right to data portability, new paragraph with more detail Section 15.10: The right to object, new paragraph with more detail Section 15.11: Rights in relation to automated decision making and profiling, re-worded paragraph. Section 20: Biometric data – removed that parents/legal guardians would have to opt out, and replaced with choosing to withhold their consent. Appendix 1: MAT Personal Data Breach Procedure has been rewritten and made an appendix. Appendix 2 and 3 have been added to provide further resources to support this policy. Throughout the policy references to residential services have been removed	HoO	Mar 2025

Person Responsible:	Group Director
Date of first draft:	February 2018
Date adopted by the Trust Board:	May 2018
Date of implementation:	May 2018
Date reviewed:	Mar 2025
Date of next review:	Mar 2027

Additional documents:

MAT Data Retention Schedule V5
MAT Data Mapping Log V5

Data Protection Policy

1. Purpose

This policy sets out the processes and procedures for ensuring that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations 2018, other relevant legislation, and best practice.

The principles set out within this policy apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

2. Scope

This policy applies to all employees and volunteers of MacIntyre Academies Trust ('MAT' or 'MacIntyre Academies') who access or use personal data that MacIntyre Academies is responsible for as Data Controller.

MacIntyre Academies employees, agency staff and volunteers are data processors and must abide by this policy.

This policy should be read in conjunction with the following other MacIntyre Academies policies:

- MAT Recruitment and Selection Policy
- MAT Whistleblowing Policy
- MAT Acceptable Use of ICT Policy
- MAT Data Breach Procedures
- MAT Artificial Intelligence (AI) Policy
- Academy Safeguarding Policies

This policy doesn't form part of any contract of employment and may be amended from time to time.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: - Name (including initials) - Identification number - Location data - Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: - Racial or ethnic origin - Political opinions - Religious or philosophical beliefs - Trade union membership - Genetics - Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes - Health – physical or mental - Sex life or sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Schedule of Responsibilities

The Trust Board	Ensure that a suitable and comprehensive policy is in place with supported procedures. Ensure that there is a suitably qualified Data Protection Officer and that the Trust comply with regulatory duties.
Group Director	Is accountable to the Trustees for the implementation of this policy and for ensuring there is strategic oversight and budget for effective data management.
Trust Data Protection Lead (Head of Operations)	Work closely and are the contract manager of the brought in services DPOiS. Is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on Trust data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
DPOiS To contact the DPO (DPOiS) 0203 961 0110 dpois@gdpr.school	DPOiS is a brought in DPO service which the Trust subscribe to. On behalf of the Trust Data Protection Lead they oversee breaches and data management activity and advise on all data management activity. DPOis is responsible for providing advice and support under this policy and advising on updating the policy as required.
Academy Principals	Academy Principals will take active steps to promote good practice under this policy, monitor and review the management and implementation of this policy in the Academy for which they are responsible. They will assign a School Data Protection Lead, most often the School Business Manager, who will take responsibility for data

	protection within their setting. The Principal, alongside the Data Protection Lead will identify training needs, ensuring competence of all staff and volunteers as they are responsible for the operation of this policy.
Academy Data Protection Lead (usually the School Business Manager)	Is responsible for co-ordination of all data protection activities in close partnership with DPOiS and the Trust Data Protection Lead.
All employees	Are responsible for: - Collecting, storing and processing any personal data in accordance with this policy - Informing the school of any changes to their personal data, such as a change of address - Contacting the DPO, via the GDPRiS system in the following circumstances: o If there has been a data breach o If there has been a significant near miss event - Contacting their Data Protection Lead in the following circumstances (the Data Protection Lead will engage the DPOiS for advice where required). o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure o If they have any concerns that this policy is not being followed o If they are unsure whether or not they have a lawful basis to use personal data in a particular way o If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK o Whenever they are engaging in a new activity that may affect the privacy rights of individuals o If they need help with any contracts or sharing personal data with third parties

5. Introduction

MacIntyre Academies Trust, or 'the Trust' collects and uses personal information about other individuals who they come into contact with. This information is processed in order to enable Academies to provide education and care, and other associated functions, including legal requirements or statutory obligations. Subsequently, in the course of their work, employees will have access to large amounts of confidential and personal information, including but not limited to information about students, staff members and others.

The Trust is responsible for the activities of all of the Academies and is therefore the legal entity responsible for the processing of personal data. The Trust is therefore the data controller for the processing and the entity subject to DPA registration obligations set out below.

As a processor of personal information, the Trust is registered with the Information Commissioners Office (ICO), and ensures that the registration is maintained.

MacIntyre Academies' ICO registration number is **ZA103532.**

A copy of the notification document is available to view at each Academy, and on ICO's website by following the link https://ico.org.uk/esdwebpages/search.

6. The UK General Data Protection Regulations

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

The UK GDPR covers the collecting and holding of information about an identifiable living individual, and its use, disclosure, retention and destruction. It gives people the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. For further information, see 'Guide to data protection' on the website of the Information Commissioners Office https://ico.org.uk/for-organisations/guide-to-data-protection/

MacIntyre Academies Trust, each Academy and every employee has a legal duty to protect the privacy of information relating to individuals that it processes.

Personal data means information about a living individual who can be identified from that information and from other information which is in, or likely to come into, MacIntyre Academies' possession.

GDPR defines 'sensitive personal data' as that related to racial or ethnic origin, political opinions or religious beliefs, trade union membership, physical or mental health condition, sexual life, and convictions, proceedings and criminal acts this information is also labelled as 'Special category data'.

The holding of sensitive personal information generally requires the explicit consent of the person; where the request received relates to a child or young person, MacIntyre Academies normally obtains this consent from parents/guardians in writing as part of its needs assessment. For young people over the age of 13 this permission is sought from them providing they are capable of making decisions about their own data. Where the person lacks the capacity to consent the ability to make a decision will fall to their parent or guardian or to whomever has parental responsibility for the student. If the student and has no representative that can give consent, a best interests decision will be made by MacIntyre Academies.

GDPR works in two ways. Firstly, it states that anyone who processes personal information must comply with principles that data should be:

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

Secondly it specifies that the data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

7. Policy Principles

MacIntyre Academies will take all practical steps to ensure that the requirements of the UK GDPR are achieved and maintained throughout the organisation at all times in accordance with the 6 enforceable principles as laid out in Article 5 of the GPDR:

Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)

Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)

Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. (accuracy)

Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. (Storage limitation)

Principle 6 (the Security Principle) - Personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data, using appropriate technical or organisational measures. (integrity and confidentiality)

GDPR also includes a 7th Principle:

Principle 7 - the Accountability Principle which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. In our Trust and in each one of our academies, the responsibility for adherence to the principles lies with all staff.

MacIntyre Academies Trust and its Academies will:

a) Demonstrate compliance with the GDPR through a range of accountability measures including Privacy Impact Assessments, Annual Data Audits, Annual Policy Review and the appointment of a dedicated Data Protection Officer.
b) Publish Privacy Notices informing why data is being collected at the point it is collected, including the legal grounds for collection.
c) Will seek consent for the processing of personal data.
d) Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.
e) Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (see section 15)
f) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
g) Adopt internal procedures for detecting, reporting and investigating a personal data breach.
h) Ensure that processes for handling personal information are only available to authorised individuals.
i) Share information with others only when it is legally appropriate to do so, utilising Information Sharing Agreements in accordance with the ICO's Data Sharing Code of Practice, where necessary.

j) Share personal data with the police or others for the purpose of crime preventions and detection, the apprehension or prosecution of offenders or for the purpose of legal proceedings, where properly requested.
k) Ensure our staff are appropriately trained and aware of and understand our policies and procedures.
l) If the academy carries out automated decision making (including profiling), comply with all the relevant requirements of the GDPR.
m) Produce an information asset register that contains details of the records it holds.
n) Check the quality and the accuracy of the information it holds
o) Ensure all staff are appropriately and regularly trained and aware of and understand the academy policies and procedures.
p) Disclose personal data where required to do so by law for example, following receipt of a court order.

8. Data Privacy Impact Assessments (DPIAs)

Privacy Impact Assessments will be carried out when planning new initiatives which involve "high risk" data processing activities i.e., where there is a high risk that an individual's right to privacy may be infringed such as monitoring or processing special categories of personal data, especially if those initiatives involve large numbers of individuals or new technologies. Such Assessments will allow us to identify and fix problems at an early stage.

9. Data Audits

Personal data will be reviewed and documented annually through a Data Audit and review of the MAT Data Mapping Log. This audit will map the flow of personal data into and out of the Trust.
The annual audit will check the accuracy of the information held. It will ensure that information is not retained for longer than is necessary, and that when obsolete information is destroyed that it is done so appropriately and securely.
Understanding data and how it is being processed is a key step to ensuring compliance with data protection principles.

10. Privacy Notices

MacIntyre Academies publishes privacy notices on its website which provide information about processing of personal data for staff, pupils and parents. Privacy Notices must be concise, transparent, intelligible and easily accessible. They must provide information about:

- The Academy and the Trust
- Contact details of the DPO
- What personal data is gathered
- The purpose of processing data and the legal basis for the processing of that data
- Who the personal data is shared with
- Transfers outside EU and how data is protected
- Retention period or criteria used to set this
- Legal rights e.g. the right to withdraw their consent to their data being used
- Right to complain

Privacy notices must be reviewed at regular intervals. Academies must issue an annual privacy notice to all parents, pupils over 18, and employees, before, or as soon as possible after, any personal data relating to them is obtained, and annually thereafter.

11. Lawful basis

GDPR sets out conditions that must be met for the processing of personal data to be lawful. At least one of these must apply whenever personal data is processed:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The Lawful basis for processing personal data is explained in relevant Privacy Notices.

12. Consent

The Academies and the Trust will seek consent to process some types of personal data that do not fall under other legal categories outlined above.

'Consent' is defined as any freely given, specific, informed indication of the data subject's wishes by which he or she, by a statement, signifies agreement to personal data relating to him or her being processed. Consent must be unambiguous and be a positive indication of agreement. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent must be freely given and capable of being withdrawn at any time. It must be as easy for an individual to withdraw their consent as it was to provide it in the first place. Clear explanation must be given to individuals what they are consenting to and of their right to withdraw consent.

Separate consents must be obtained for specific processing operations. It must be distinguishable from other matters and not "buried" in wider written agreements.

13. Retention and Security of Personal Data

MacIntyre Academies will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule. We will ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure, making certain that only authorised individuals have access to personal data.

Cloud based technologies are utilised; following completion of a data privacy impact assessment prior to implementation, appropriate security measures are in place to secure this data including files being saved in an encrypted form requiring username and password to log into the service to decrypt the files for access.

Data is retained in accordance with our data retention schedule which is available on our website.

14. Personal Data Breaches

The document Appendix 1 Personal Data Breach Procedure contains more detail.

The following bullet points are key points for quick reference.

- All data breaches or suspected data breaches, or significant near miss data events must be logged electronically on the GDPRiS system.
- In assessing how serious a data breach is the Data Protection Lead and DPOiS will consider how much the released data is likely to put the individual's rights and freedoms at risk.
- Where a breach is reportable to the ICO the academy will inform the Head of Operations. With sign off from the Group Director, the breach will then be reported to the ICO centrally. Academies must not report breaches directly to the ICO.

Useful resources: Appendix 2: Actions to minimise the impact of breaches
Appendix 3: Examples of a Personal Data Breach

15. Your rights under GDPR:

15.1 The right to be informed

Individual data subjects have the right to be informed about the collection and use of their personal data. See section 11 Privacy Notices

15.2 The right of access

Individual data subjects will have the right to know exactly what information is held about them and how it is processed.

There are two distinct rights of access to information held by schools about children, parents and staff:

- Under the UK GDPR any individual has the right to make a request to access the personal information held about them.
- The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005.

15.3 Subject Access Requests (SAR)

UK GDPR gives individuals the right to access personal data relating to them processed by a data controller. Requests may be received by employees, current or past, or by pupils or their parents.

A SAR can be made verbally or in writing. A non-mandatory SAR Request Form is available on request should the data subject wish to use it. The form is a way for the school to gather all relevant information necessary to complete and subject requests. Where a SAR is made verbally, the Data Protection Lead, or person receiving the SAR will populate the form on the requestors behalf.

When a request is received it will be logged with DPOiS for processing by the Data Protection Lead.

Where the original request does not clearly identify the information required, then further enquiries should be made.

Where a request received does not mention the GDPR or SAR, where this meets the criteria this will still be processed as such.

The identity of the requestor will be established before the disclosure of any information is made proof of the relationship with the child (if not known) must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child.

Below are some examples of documents which can be used to establish identity:

- Passport
- Driving licence
- Utility bill with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement.

All SARs received will be responded to within one month (irrespective of school holiday periods). The month will not commence until after receipt of proof of identity and any necessary clarification of information is sought.

There are some exemptions available under the GDPR, which mean that occasionally personal data will need to be redacted (blacked out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosures to ensure that the intended disclosure complies with MacIntyre Academies' legal obligations.

Where the personal data also relates to another individual who can be identified from the information the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding

the information from disclosure. These considerations can be complex and additional advice will be sought where necessary.

Any information which might cause serious harm to the physical or mental health or emotional condition of the child, or another person will be withheld along with any information that would reveal that the child is at risk of abuse, or information relating to Court Proceedings.

Where an exemption is used, it will be recorded as well as the justification for using the exemption, this will be provided to the requester when appropriate to do so.

15.4 Requests from Pupil / For Pupil data

Children can exercise their rights under the GDPR once they are considered capable of making decisions by the academy. The right can be exercised by a person with parental responsibility on behalf of their child if the child is not able to understand the process or has not reached sufficient maturity.

If a child's competency is brought into question by the Legal Guardians or the Academy, the final decision will be made by the Executive Leader for Education and Care, who will take into account the views of the Academy SENCO, information on the students file, as well as speaking with the child's class team and trusted adults and if needed talk with them to make the decision if the child is competent enough.

For the purposes of a SAR, MacIntyre Academies will apply the full legal definition of 'parental responsibility' when determining who can access a child's personal data. Proof of the relationship with the child must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child.

The ability of young people to understand and exercise their rights is likely to develop or become more sophisticated as they get older. It is widely accepted that children of primary school age do not have the maturity to understand or exercise their own rights; and in accordance with guidance from the Information Commissioners Officer https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-uk-gdpr/ indicate as a general guide, a child of 12 or older is expected to be mature enough to understand the request they are making.

A child may, of course, be mature enough at an earlier age or may lack sufficient maturity until a later age, and so requests received by MacIntyre Academies for data relating to a child/young person will be considered on a case-by-case basis considering the circumstances surrounding the case and the child.

Where a SAR is received by a person with parental responsibility on behalf of a child over the age of 12 and MacIntyre Academies considers the child is mature enough to understand their rights, MacIntyre Academies will seek permission from the child for information to be given to the parent before it's disclosed. MacIntyre Academies, will, where appropriate, discuss the request with this child in question to ensure they understand rather than relying on a signature. A child with competency can refuse to consent to a request for their personal information made under the Data Protection Act. This position differs when the request is for access to the Education Record of their child (see below for more detail).

15.5 Request for Access to a curricular and education record as defined within the Education (Pupil Information) (England) Regulations 2005.

A parent may make a request to access information contained within their child's education record, regardless of whether the child agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the child.

For the purpose of responding to an Educational Records request, the Academy will apply the definition of 'parent' contained within the Education Act 1996.

An "educational record" means[1] any record of information which:

a) Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local education authority and any special school which is not so maintained.

b) Relates to any person who is or has been a pupil at any such school; and
c) Originated from or was supplied by or on behalf of the persons specified in paragraph

Other than information which is processed by a teacher solely for the teacher's own use.
The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Schedule to the Data Protection (subject access) (Fees and Miscellaneous Provisions) Regulations 2000.
No charge will be made to view the education record.
The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days).
An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the child or another person or if the disclosure of the information would reveal that the child is at risk of abuse.
There is no obligation for the Academy/Trust to respond to requests made this way, if the Data Protection Lead feels that a SAR would be a more appropriate form of request, due to the data being requested, they will contact the requester and confirm that the request can proceed as a SAR, or, dismiss the request.

15.6 The right to rectification

UK GDPR includes the right for individuals to have inaccurate personal data rectified or completed if incomplete. Requests should be made in writing to the Trust Data Protection Lead who will liaise with DPOiS and respond within 30 days of receipt. Where any requests are received verbally, they will be asked to complete these in writing. Upon receipt of the request the Trust Data Protection Lead will liaise with DPOiS to investigate whether the data held in question is accurate. During this time, access to data which is being contested will be restricted, wherever possible. A note will be placed on the system/file that the information is being reviewed for accuracy. If data is found to be accurate, the individual will be informed that this will not be amended and will be notified of their right of complaint to the ICO. The file note will be updated to include that the data has been reviewed for accuracy. There may be some exemptions to the right to request rectification such as where these are manifestly unfounded; or excessive. Each request will be considered on a case by case basis and in line with guidance from the ICO. Requests for rectification will be added to the MAT Record of Requests Log.

15.7 The right to erasure

Individuals have the right to request that personal data is erased; sometimes termed 'the right to be forgotten.' Requests should be made in writing to the Trust Data Protection Lead who will liaise with DPOiS and respond within 30 days of receipt. Where any requests are received verbally, they will be asked to complete these in writing. Upon receipt of the request the Trust Data Protection Lead will liaise with DPOiS to investigate whether the request meets the criteria to be considered for erasure; i.e. if the holding of data is no longer necessary; where the legal reason for holding such data is explicit consent and the consent is withdrawn, where the data is held for purposes of direct marketing or where the data is being processed unlawfully. Where the data is erased from MacIntyre Academies' systems/records; reasonable attempts will also be made to inform other organisations who may hold this data, as disclosed by MacIntyre Academies. There may be some further exemptions to the right to request rectification such as where these are manifestly unfounded; or excessive. Each request will be considered on a case by case basis and in line with guidance from the ICO. Requests for erasure will be added to the MAT Record of Requests Log.

15.8 The right to restrict processing

The right to restrict processing allows individuals to request the limitation of the processing of their personal data under certain circumstances. In line with UK GDPR regulations, a data subject can exercise this right when they contest the accuracy of their data, when the processing is unlawful but they oppose erasure, or when they need the data to establish, exercise, or defend legal claims.
Additionally, an individual may request a restriction if they object to processing based on legitimate interests, pending the verification of the grounds for such processing.
During a period of restriction, the personal data will be stored but not processed, and the data subject will be informed before any processing is resumed.
The Data Protection Lead will track the activity on DPOiS.
MacIntyre Academies is committed to honouring this right and will ensure that any request for restriction is promptly addressed in accordance with the relevant data protection laws.

15.9 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data across different services.
In accordance with UK GDPR, data subjects have the right to request a copy of their personal data in a structured, commonly used, and machine-readable format. They can also request that their data be transferred directly to another organisation, where technically feasible. This right applies when the processing is based on consent or a contract and is carried out by automated means.
MacIntyre Academies is committed to facilitating this right by providing individuals with easy access to their personal data and supporting secure transfers to other schools, colleges or any such entity upon request, in compliance with the applicable data protection laws.

15.10 The right to object

The right to object allows individuals to challenge the processing of their personal data in certain circumstances. Under UK data protection laws, individuals have the right to object to the processing of their personal data when it is based on legitimate interests or the performance of a task in the public interest, including profiling.
This right also applies to direct marketing, where individuals can object to their data being used for such purposes at any time. Upon receiving an objection, MacIntyre Academies will cease processing the personal data unless there are compelling legitimate grounds, which can be evidenced, for the processing that override the individual's interests, rights, and freedoms.
MacIntyre Academies will also respect any objection related to direct marketing and ensure that such processing is immediately stopped.
The Trust is committed to ensuring that data subjects can exercise their right to object in a straightforward and transparent manner.

15.11 Rights in relation to automated decision making and profiling.

Under UK data protection laws, individuals have specific rights in relation to automated decision-making and profiling, particularly where decisions are made solely based on automated processing of personal data, including profiling, and have legal or similarly significant effects.
MacIntyre Academies Trust seeks to ensure that no individual is subject to a decision based solely on automated processing.
In cases where automated decision-making may rarely occurs, individuals have the right to request human intervention, express their point of view, and challenge the decision.
MacIntyre Academies is committed to maintaining transparency and fairness will ensure that individuals are informed if ever such processes are being used, in compliance with applicable data protection regulations.

15.12 Transfers to Third Parties

Requests for data received from third parties, which are not a legal requirement, such as mortgage companies asking for salary information will be logged as a request on the MAT Record of Information Request Log by the relevant School Business Manager and an

overview of responses made. Prior to any information being provided, MacIntyre Academies will seek to verify that consent has been provided by the individual.

15.13 Third Party Suppliers

MacIntyre Academies will ensure that any third parties which process data on its behalf ('data processors') meet the requirements set out in article 28 of UK GDPR. Supplier contracts where the trust passes data to them, and they receive and store it, such as insurers, payroll and curriculum enrichment providers, are data processors. The Trust Data Protection Lead is responsible for ensuring that these are compliant with the GDPR and uses GDPRiS to achieve this.

At each Academy the School Business Manager will ensure that all such third-party suppliers are compliant with data clauses as detailed in paragraph 3 of article 28. A check list taken from this section of the GDPR is included in Appendix 4 – Third Party Processor – Supplier Contracts Checklist.

16. Staff Data Protection Training

MacIntyre Academies Trust will take organisational steps to keep personal data secure, and the deployment of staff data protection training is key to reducing the likelihood of data losses. Academies will ensure that new starters will receive data protection training, proportionate to their role, before they have access to personal data and existing staff will receive regular and refresher training.

Course	Induction	Frequency of repetition	Variations
GDPR UK: Education	Yes	2 years	All staff, all volunteers
GDPR UK: Advanced	Yes	3 years	Data Protection Leads
GDPR role specific modules as defined by local Data Protection Lead	No	Termly	Key data processers

17. CCTV

Refer to the MAT CCTV Policy.

18. Call recording

Academies may choose to introduce call recording on their switchboard system for incoming / outgoing calls. Where this is the case, a clear proposal must be used for communication with stakeholders, and consultation with parents and staff must be considered. The following points must be followed:

a) A clear alert to callers that their call will be recorded must be included
b) A notice explaining why calls are recorded and for how long the calls will be stored for must be posted on the academy website and linked to Privacy notices.
c) Access to recordings of calls must be restricted to the Principal, the School Business Manager and one other nominated member of staff where desired.

19. Photographs and Electronic Images

Further information in relation to the use of photographs/videos that contain images of children can be found in MacIntyre Academies' Acceptable Use of ICT Policy which all employees sign up to and within Safeguarding Policies. Each school has a policy that provide the Academy's position regarding parents photographing and filming children at Academy events and the use of images of children by the Academy in any publicity material, its website, in newspapers and in outside agency publications.

20. Biometric Data

If an Academy uses or intends to use biometric data (such as fingerprint technology) a separate, detailed notice will be sent to all children and parents explaining the intended use and providing parents with options for alternative systems if they choose to withhold their consent. Any Academy in the Trust will obtain the written consent of at least one parent or legal guardian before taking and using and biometric data from a child.

21. Record Management

MacIntyre Academies is committed to the responsible management of all records, both physical and electronic, created by the trust and the academies, including records that third parties manage on behalf of the Trust.

Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy, or electronic format e.g., paper documents, scanned documents, e-mails which document business activities and decisions, audio and video recordings, text messages, notes of telephone and Skype conversations, spreadsheets, word documents, presentations etc.

Individual employees must ensure with respect to records for which they are responsible that they:

a) Manage the records consistently in accordance with the Trust and Academy policies and procedures
b) Properly document actions and decisions taken
c) Hold personal information securely
d) Only share personal information appropriately and do not disclose it to any unauthorised third party
e) Dispose of records securely in accordance with the MAT Data Retention schedule.

21.1 Storage of records

All systems and records must have designated owners throughout their lifecycle, whether that is named individuals or nominated business areas.

Records must be stored in environmental conditions that protect them from deterioration.

Digital continuity must be considered for the systems and formats that are used to store digital records. All records must be traceable and retrievable.

21.2 Disposal of records

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained when there is a requirement to do so. Under UK GDPR and the DPA 2018, personal data processed by MacIntyre Academies must not be retained for longer than is necessary for its lawful purpose.

The default standard retention period for MacIntyre Academies is stated on the MAT Data Retention Schedule according to the type of record. The person responsible for the disposal of the records is noted on the schedule.

Records must only be retained beyond the stipulated period if their retention can be justified for statutory, regulatory, legal or security reasons.

Processes must be in place to ensure that records pending audit, litigation or investigation are not destroyed.

Processes must be in place to ensure that all backups and copies are included in the destruction of records, or that data is put beyond use.

21.3 Methods of disposal

Records containing personal data should be made either unreadable or un-reconstructable. This means:

The provision of a shredder is essential for disposal of highly sensitive information.

- Shred paper records using a cross-cutting shredder
- Cut CDs, DVDs and floppy disks into pieces
- Dismantle and shred audio or video tapes and fax rolls
- Dismantle and sand hard disks
- Use a wastepaper merchant to bundle up and dispose of any other records
- Do not put records containing personal data in with the regular waste or in a skip unless there is no other alternative.

Confidential Waste Bins. Due consideration must be given to the confidentiality where confidential waste bins are in place and staff must be aware that highly sensitive documents should be disposed of by immediate shredding and not placed in the Confidential Waste Bin. Where Confidential Waste Bins are used the Principal must sign off the procedure for key management and retrievals.

22. Breaches of this Policy

MacIntyre Academies understands that data breaches do sometimes occur, even when best efforts to prevent them are made. This policy requires employees and volunteers to be honest and timely in reporting such data breaches when they happen, and to take actions to prevent recurrence in agreement with the Data Protection Officer.

All breaches of confidentiality and information security, actual or suspected, will be reported and investigated under MacIntyre Academies' Disciplinary Policy and Procedure. In accordance with the MAT Disciplinary Policy, serious breaches of the Data Protection Policy will normally be regarded as gross misconduct.

An employee's conduct and/or actions may also be unlawful or illegal and they may be personally liable. MacIntyre Academies reserves the right to report any illegal violations to the appropriate authorities

23. Data Protection Policy Review

The MAT Data Protection Policy will be reviewed every 2 years, or earlier when required, and published on Academy websites. Policies intended to be read by children will be explained in clear non–technical language and in a way that can be readily understood.

24. Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong. You can make a complaint at any time by contacting our data protection officer (see section 10 for contact details).

You can also complain to the Information Commissioner's Office in one of the following ways:

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

Historic updates table:

Version Number	Purpose/ Change	Responsibility	Date
V2	Change of title to Trust Finance Officer to Trust Business Manager. Change of title for Chief Operating Officer to Chief Executive Officer. Adding in telephone number, email, name of DPO in section 10 The School Business Manager is responsible for ensuring the compliance of third-party suppliers where they are data processors (section 16)	CEO	5th June 2019
V3	Change of name of DPO from Helen Coombs to Jo Godding	CEO	17th October 2019
V4	Section 16 - Requests for Rectification added. Section 17 added – Requests for Erasure. Section 18 added – Transfers to Third Parties added. Renumbering of previous sections 16 onwards. Section 23 - CCTV – now includes reference to local policy on school websites. Section 26 – complaints procedure included	CEO	9th January 2020
V5	Section 3 - Change to DPO from Trust Business Manager to DPOiS and review of responsibilities – TBM now works in conjunction with DPOiS Section 15.1 – Change to procedure for logging SAR – now online using GDPRiS Section 16 – change to contact procedures – via DPOiS Section 17 – change to contact procedures – via DPOiS Section 20 – change to procedures – online GDPRiS	CEO	30th April 2020
V6	Section 14 - Wording added on cloud storage	CEO	8th October 2020
V7	The role of CEO is now incorporated into the role of the Group Director for Education and Children's Services. The role of the Trust Business Manager has been updated to the Trust Data Protection Lead, which will be performed by the Head of Operations. Section 6: Clarification of the Principles of GDPR Section 6: Addition of points l,m,n,o,p Section 10: Updated Contact details for Data Protection Officer Section 11: Re-wording and grouping of sections relating to an individual's rights under GDPR. Section 18: Overlap with Data Breach Procedure removed and some key points stated.	Group Director	Oct 2021
V8	Updated to reflect UK GDPR / The Data Protection Act 1998 throughout Updated links to ICO and Clarification that the Head of Operations is the Data Protection Lead Referred to MAT CCTV Policy and section in this policy Referred to MAT Surveillance & Remote Monitoring Policy Added Section 22: Call recording Added Section 25: Previously MAT Record Management Policy (now retired) Point of clarification Section 26 Listed staff training in relation to GDPR	Group Director	March 2023
V9	Updated that any data breach reportable to the ICO is dealt with by the Head of Operations and their team, with the oversight of the Group Director	Group Director	October 2023

(for most recent updates see front cover)

Appendix 1: Personal Data Breach Procedure

On discovering a Breach…

a) On finding or causing a breach or potential breach:

- **Staff** member must immediately notify the data protection officer (DPO) by logging the breach on the GDPRiS system. If for any reason they are unable to do this, they should alert the Principal or the most senior member of staff on site, without delay.
- **Volunteer / Agency staff** must email data.protection@macintyreacademies.org and their school business manager. They should seek advice immediately from the most senior person on site.

b) DPOiS will investigate the report, with the support of the Academy Data Protection Lead, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

c) Employees, governors and volunteers, will be asked to co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

d) If a breach has occurred or it is considered to be likely that is the case, the Academy Data Protection Lead will alert the Academy Principal. The Trust Data Protection Lead will have a notification of all breaches recorded via the GDPRiS system. Where the breach is of a serious nature the Group Director and Board will also be informed.

e) DPOiS and the Data Protection Lead will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help with this where necessary, and external advice will be sought when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)

f) The DPOiS and Data Protection Lead will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences

g) DPOiS will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

h) Decisions and evidence is documented on the GDPRiS system throughout the process, from the breach to the final conclusion.

i) Where the ICO must be notified, the Trust Data Protection Lead will do this, under the expert advice of DPOiS, via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the Trust Data Protection Lead will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the Trust Data Protection Lead and the brought in DPO services from DPOiS.
- 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

j) If all the above details are not yet known, as much as can be reported will be submitted within 72 hours of the initial awareness of the breach. The report will explain what information will follow and why there is a delay.

k) Where the Trust is required to communicate with individuals whose personal data has been breached, the Trust Data Protection Lead will coordinate this via the most suitable route, in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the Trust Data Protection Lead
- 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

l) The Trust Data Protection Lead, in partnership with DPOiS, and the Group Director, will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, the Risk Protection Arrangement, banks or credit card companies

m) 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)

n) DPOiS and Data Protection Leads will meet to review what happened and how it can be stopped from happening again, other colleagues will be invited to attend the reflection to ensure it encompasses all relevant perspectives. This meeting will happen as soon as reasonably possible.

o) The Trust Data Protection Lead will meet with the DPOis on an annual basis, or more frequently where required, to assess recorded data breaches and identify any trends or patterns requiring action by the Trust to reduce risks of future breaches.

p) Academy Data Protection Leads meet and discuss GDPR at half termly Ops Forum meetings, where GDPR is a standing agenda item.

Appendix 2 Actions to minimise the impact of data breaches

This appendix provides examples of steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

Scenario A:

Special category data (sensitive information) is accidentally made available via email to unauthorised individuals

a) The sender must attempt to recall the email as soon as they become aware of the error

b) Employees who send personal data in error must report this on GDPRiS and, when a serious matter, inform the Data Protection Lead verbally, as soon as they become aware of the error.

c) If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Colwyn/Nexus Helpdesk to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

d) In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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

e) The Data Protection Lead will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

f) The Data Protection Lead will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

g) If safeguarding information is compromised, the Designated Safeguarding Lead and Group Director will be informed. At the soonest opportunity key personnel will meet and discuss whether the Trust should inform any, or all, of its 3 local safeguarding partners

Scenario B:

Details of pupil premium interventions for named children being published on the school website

a) A Website administrator must removes the information from the website

b) The Academy Data Protection Lead must liaise with DPOiS and investigate the extent of the breach and the possible harm that may be caused to the data subject.

c) DPOiS will advise where contacting the data subjects to inform them and apologies for the breach is required.

d) The investigation will inform what further mitigations may be required. Examples may be training for website administrators, or a new protocol for sign off of documents to upload.

Scenario C:

Hardcopy reports sent to the wrong pupils or families

a) Immediate actions are taken to retrieve any reports which could contain further breaches that have not yet been delivered. This may entail halting post leaving the office, or retrieving envelopes from pupils due to leave the school site.

b) The Data Protection Lead investigates how the breach has occurred and assesses the breadth of the error.

c) Communication is sent out to parents by email, or if a small number only, by phone call:

- Alert parents/carers of the breach
- Politely request that they do not open the envelope
- Make a plan for how to best and most securely retrieve the hardcopy.

d) Depending on the practicalities, employees may make home visits to retrieve envelopes

e) Where there has been a breach, DPOiS will support the Academy Data Protection Lead to notify the data subjects.

f) The investigation and reflective exercises will ensure that mitigations are put in place to prevent re-occurrence.

g) Case studies will be shared across the Academies in the Trust to ensure that the breaches bring around better practice for all.

Appendix 3 - Examples of a Personal Data Breach Incident

Theft / loss incident:

- Of data – written or electronically held
- Of equipment – for example laptops, mobile phones or tablets, USB Drives or SD cards.

Accidental incident:

- Sending an email containing sensitive information to the wrong email address.
- Sending an email containing sensitive information to 'all staff'.

Malicious incident:

- Social engineering / blagging – e.g., unknown people asking for information which would enable access to data (e.g. a password or details of someone).
- Unauthorised disclosure of information verbally, electronically or in paper form
- Falsification of records, inappropriate destruction of records.
- Unauthorised information access or use

Access Violation:

- Disclosure of login details or passwords to unauthorised people, e.g., writing down your password and leaving it on display.
- Accessing systems using someone else's authorisation e.g., their user id, password or security token
- Allowing unauthorised physical access to secure premises or areas
- Leaving sensitive information (on paper or screen) visible on an unattended desk.

IT incident

- Denial-of-service attack (a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet).
- Computer infected by a virus or other malware, e.g., spyware.

Environmental incident:

- Damage caused by natural disasters e.g., fire, burst pipes, flooding.
- Deterioration of paper records or backup tapes.

Inappropriate Use:

- Using a new supplier without premission
- Inappropriate use of Artificial Intelligence (AI) – for example, uploading personal information to generative AI tools.
- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Personal use of services and equipment in work time

Appendix 4 – Third Party Processor – Supplier Contracts Checklist

Supplier contracts - GDPR checklist

Under the General Data Protection Regulation (GDPR) you must ensure that any third parties that process data on your behalf meet the GDPR requirements

- To do this, check the data protection clauses in all contracts that were live when the GDPR came into force (25 May 2018), and any that you've entered into since then
- You must include certain information in contracts with third parties/suppliers (such as insurers, payroll and school club providers) where the school passes data to them, and they receive and store it
- You can add this information as a schedule to the contract, rather than having to amend the whole document
- Our checklist sets out the information that the schedule needs to cover to help you get GDPR-compliant. Use it when amending contracts to make sure you're covering every base. You can also use this when agreeing new contracts
- The information in the checklist is taken from paragraph 3 of article 28 of the GDPR
- Speak to your legal advisers for further support and advice on the process of updating contracts

Supplier contracts – GDPR checklist

INFORMATION TO INCLUDE TO MEET GDPR REQUIREMENTS	COMPLETE?
The subject matter, duration, nature and purpose of the data processing *this information will need to be specific to each contract*	☐
The type(s) of personal data being processed *this information will need to be specific to each contract*	☐
The categories of the data subjects (the individuals whose data is being processed) *this information will need to be specific to each contract*	☐
The obligations and rights of the data controller (your school) *this information will need to be specific to each contract*	☐
The data processer (the third party/supplier) processes data only on the documented instructions of the school	☐
The people who process the data are committed to confidentiality, or are required by law to uphold confidentiality	☐
The third party takes measures to ensure data is processed securely	☐
The third party will not engage another processor without prior written authorisation from the school	☐
If the third party does engage another processor, this processor will be bound by a written contract with the same data protection conditions as are in the contract with the school	☐
The third party helps the school comply with: • Upholding the data rights of individuals • Secure processing • Reporting and communicating data breaches • Conducting impact assessments where relevant	☐
The third party deletes or returns the personal data to the school at the end of the provision of services (unless the law states that the information must be kept)	☐
The third party makes information available to the school to demonstrate its compliance with the obligations in the contract, and allows the school or another party instructed by the school to conduct audits and inspections	☐