South Pennine Academies

Data Protection Policy (Inc. GDPR)

Date of Next Review:	June 2027
Date of Implementation:	April 2024
Date Approved by Trustees:	April 2024
Policy Reviewer:	Operations Director

Contents

1. Statement of intent

Our academy is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the data protection legislation.

The academy may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

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

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

2. Legal framework

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

- The General Data Protection Regulation (GDPR) 2018
- The Freedom of Information Act 2000
- The Education (Student Information) (England) Regulations 2005 (as amended in 2018)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Act 2018
- Electronic Commerce (EC Directive) Regulations 2002
- Protection of Freedoms Act 2012
- DfE (2023) Keeping Children Safe in Education 2023

This policy will also have regard to the following guidance:

- ICO (2012) IT asset disposal for organisations
- ICO (2022) Guide to the General Data Protection Regulation (GDPR)
- DfE (2023) 'Data Protection toolkit for schools

This policy will be implemented in conjunction with the following other academy policies:

- Photography and Videos at School Policy
- E-security Policy
- Freedom of Information Policy
- CCTV Policy
- Records Management Policy

3. Applicable data

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

Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data' and is defined as:

- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Personal data which reveals:
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Principles

'sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, academies are only able to process this if it is either:

- Under control of official authority; or
- Authorised by domestic law

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or excercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

4. Principles

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by UK 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.

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

5. Accountability

Our academy will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in UK GDPR.
The academy will provide comprehensive, clear and transparent privacy policies.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional
- Could result in a risk to the rights and freedoms of individuals
- Involve the processing of special categories of data or criminal conviction and offence data.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The academy will also document other aspects of compliance with UK GDPR where this is deemed appropriate.

Information required for privacy notices, e.g the lawful basis for processing
Records of consent
Controller – processor contracts
The location of personal data
Data Protection Impact Assessment Reports
Records of personal data breaches

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

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

Data protection impact assessments will be used, where appropriate.

6. Data protection office (DPO) / Data Security Manager (DSM) / Data Safety Officer (DSO)

A DSM will be appointed by the Trust in order to:

- Inform and advise the academy and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the academy's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing or arrange the required training to staff members.
- Arrange external compliance checks
- Cooperate with the ICO and act as point of contact

South Pennine Academies have an outsourced DPO service – GDPR Sentry who can be contacted on Telephone: 0113 804 2035 | Email: info@gdprsentry.com

GDPR Sentry will act as DPO and advisory service for all data protection matters.

Angie Green Operations Director has been appointed as Data Security Manager, she can be contacted on 01484 503110, agreen@spacademies.org

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

The DSM will report to the highest level of management at the Trust, which is the CEO and Trust Board.

The DSM and DSO will operate independently and will not be dismissed or penalised for performing their task.

Sufficient resources will be provided to the DSM to enable them to meet their GDPR obligations.

Academies will appoint a data safety officer (DSO) to be the data protection lead within the academy

7. Lawful processing

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

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

- The consent of the data subject has been obtained.

Processing is necessary for:

- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.

- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the academy in the performance of its tasks.)

Sensitive data will only be processed under the following conditions:
- Explicit consent of the data subject
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.

Processing is necessary for:
- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with law

When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

8. Consent

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

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

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

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

Consent can be withdrawn by the individual at any time.

Where the academy opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined, the academy obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children.

In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the academy on a case-by-case basis, taking into account the requirements outlined

9. Sharing data without consent

The academy may share information without consent in specific circumstances. To determine whether information can be shared without consent, the academy will identify one of the other lawful bases for processing:

- **Contract** – the processing is necessary for a contract held between the academy and individual, or because the individual has asked the academy to take specific tests before entering into a contract.
- **Legal obligation** – the processing is necessary for the academy 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 the academy to perform a task in the public interest or for it's official functions, and the task or function has a clear basis in law.
- **Legitimate interests** – the processing is necessary for the academy's legitimate interests or the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests.

Where the academy is able to justify one of the lawful bases outlined in section 7, an exemption applies, or there is a requirement under another law, information may be shared without consent.

Specifically, the GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe, and information may be shared without consent if to gain consent would place a child at risk.

10. The right to be informed

Adults and children have the same right to be informed about how the academy used their data. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

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

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

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

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

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

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

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

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

11. The right of access / subject access requests

Individuals have the right to obtain confirmation that their data is being processed. Individuals, including children, have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

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

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

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

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

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

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

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

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

In the event that a large quantity of information is being processed about an individual, the academy will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification is received.

The academy will ensure that information released in response to a SAR does not disclose personal data of another individual. This could involve omitting elements from the response to protect another individual's personal data or rejecting requests that cannot be fulfilled without disclosing another individual's personal data, unless consent has been granted from the other individual or it is reasonable to comply without their consent. The individual who made the request will be given an explanation as to why the SAR could not be responded to in full.

12. The right of rectification

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

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

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

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Requests will be investigated and resolved, where appropriate, free of charge; however, the academy may impose a reasonable fee to cover administration costs of complying with requests that are manifestly unfounded, excessive or multiple requests at once. The academy reserves the right to refuse requests that are manifestly unfounded, excessive or if exemptions apply.

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

13. The right to erasure

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

Individuals, including children, have the right to erasure in the following circumstances:

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

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

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

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

Requests for erasure will be handled free of charge; however, the academy may impose a reasonable fee to cover the administration costs of complying with requests that are manifestly unfounded or excessive or multiple requests at once.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the academy will inform other organisations who process the personal data to erase links to and copies of the personal data in question

14. The right to restrict processing

Individuals, including children, have the right to block or suppress the academy's processing of personal data.

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

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

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

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

The academy will inform individuals when a restriction on processing has been lifted.

The academy reserves the right to refuse requests for restricting processing if they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reason behind it, as well as their right to complain to the supervisory authority and judicial remedy, within one month of the refusal.

15. The right to data portability

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

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

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

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

The academy will provide the information free of charge.

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

The academy is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

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

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

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

16. The right to object

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

Individuals have the right to object to the following:

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

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

- An individual's grounds for objecting must relate to his or her particular situation.
- The academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defense of legal claims, or, where the academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.
- The academy will respond to objections proportionately, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The academy will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.

Where personal data is processed for research purposes:

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

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

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

Details of objections will be recorded with clarification of the specific objection. The requests will be responded to within one month; this can be extended by a further two months if the request is complex or repetitive. If there is no action taken to the objection, the academy will, without delay and within one month, explain the reason for this and inform them of their right to complain to the supervising authority.

17. Automated decision making and profiling

The academy will only ever conduct automated decision making with legal or similarly significant effects if the decision is necessary for entering into or performance of a contract, authorised by law and based on the individual's explicit consent.

The academy will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

When automatically processing personal data for profiling purposes, the academy will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The academy has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of law.

18. Privacy by design and privacy impact assessments

The academy will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the academy has considered and integrated data protection into processing activities.

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

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

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

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

High risk processing includes, but is not limited to, the following:
- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

The academy will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

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

19. Data breaches

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

The Principal will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

Where a breach takes place the DPO must be notified immediately. This should be recorded on GDPR Sentry and the DSM will review the breach, consulting with GDPR Sentry as required.

Where a breach is likely to result in a risk to the rights and freedoms of an individuals, the relevant supervisory authority will be informed. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the academy becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the academy will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

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

Effective and robust breach detection, investigation and internal reporting procedures are in place at the academy, which facilitate decision-making in relation

to whether the relevant supervisory authority or the public need to be notified. The Academy will document all facts regarding the breach, the effects of the breach and all actions taken. The academy will work to establish the cause of the breach and assess how a recurrence can be prevented, for example mandatory training where human error was the cause.

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

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

When notifying an individual about a breach to their personal data, the academy will provide specific and clear advice about what to do to protect themselves and their data, when possible and appropriate to do so.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

20. Data security

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access and not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks/external hard drives will not be used to hold personal information. If a member of staff wishes to access personal data off site they must upload to Microsoft 365 and only safe the documents to their work computer or M365 account.

All electronic devices are password-protected to protect the information on the device in case of theft. Where possible, the academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff and governors will not save academy/trust information on their personal laptops or computers.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

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

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

Any emails copied to personal email addresses must be blind carbon copied (bcc). So email addresses are not disclosed to other recipients.

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

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the academy premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:
- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

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

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

Our academy takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Trust IT team is responsible for continuity and recovery measures are in place to ensure the security of protected data.

21. Publication of information

Our academy publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:
- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

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

Our academy will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

22. CCTV and photography

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

The academy notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

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

The academy will always indicate its intentions for taking photographs of students and will retrieve permission before publishing them.

If the academy wishes to use images/video footage of students in a publication, such as the academy website, prospectus, or recordings of academy activities, written permission will be sought for the particular usage from the parent of the student.

Precautions, as outlined in the photography and videos at school policy are taken when publishing photographs of students, in print, video or on the academy website.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR. The academy asks that parents and others do not post any images or videos which include any children other than their own on any social media, or otherwise publish those images or videos.

23. Data retention

Data will not be kept for longer than is necessary, and will be disposed of in line with the data retention and disposal policy.

Unrequired data will be deleted as soon as practicable.

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

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

24. DBS data

All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

25. Cloud Computing

For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

All files and personal data will be encrypted before they leave a school device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DSM immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

The school's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DSM and IT team. The DSM and IT team will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the principles of the UK GDPR and DPA. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DSM / DSO / IT Team will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a timescale in line with the school's Data Protection Policy.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the school decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the school is prepared to accept that risk.

- Monitor the use of the school's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the principal

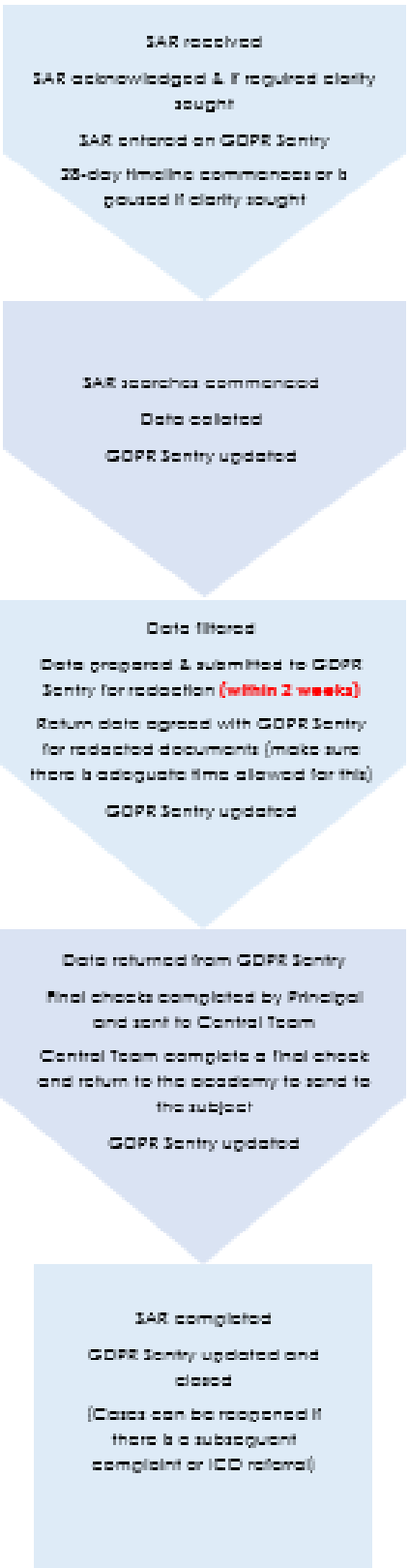
26. Policy review

This policy is reviewed every three years by the Operations Director and the Board of Trustees

The next scheduled review date for this policy is January 2027.

27. Appendix

27.1 SAR process flowchart


SAR received
SAR acknowledged & if required clarity sought
SAR entered on GDPR Sentry
28-day timeline commences or is paused if clarity sought
SAR searches commenced
Data collated
GDPR Sentry updated
Data filtered
Data prepared & submitted to GDPR Sentry for redaction (within 2 weeks)
Return date agreed with GDPR Sentry for redacted documents (make sure there is adequate time allowed for this)
GDPR Sentry updated
Data returned from GDPR Sentry
Final checks completed by Principal and sent to Central Team
Central Team complete a final check and return to the academy to send to the subject
GDPR Sentry updated
SAR completed
GDPR Sentry updated and closed
(Cases can be reopened if there is a subsequent complaint or ICO referral)