

Salendine Nook High School (Academy)

Data Protection Policy (STATUTORY) **GB free to determine how to implement**

Date policy written:	July 2022
Produced by:	Mrs V Wood
Approved by Governing Body:	Finance, Staffing & General Purposes Committee 14.7.22
Review date:	July 2023

Statement of intent

Salendine Nook High School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially social services.

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

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

Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing board

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

All staff

Staff 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 Director of Finance & Resources in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
 - 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
 - If there has been a data breach
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
 - If they need help with any contracts or sharing personal data with third parties

Legal framework

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

- The 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](#)
- [Data Protection Act 2018 \(DPA 2018\)](#) It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).
- [Protection of Freedoms Act 2012](#)
- It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

The Education (Pupil Information) (England) Regulations 2005

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

- Responsible Use of ICT and Internet Policy
- Freedom of Information Policy

Applicable data

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, such as an IP address. The 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 GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act 2018 and the test guidance from the ICO. These specifically include the processing of genetic data, biometric data, data concerning health matters, religious beliefs, criminal records, ethnic origin and union membership.

Principles

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

Accountability

Salendine Nook High School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy notices.

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

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 school will implement measures that meet the principles of data protection by design and data protection by default, including, but not restricted to:

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

Data protection impact assessments will be used, where appropriate.

Data Protection Officer (DPO)/Responsible Person

The Responsible Person will:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school'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 the required training to staff members.

An external provider has been appointed to the role of DPO at Salendine Nook High School.

On a day to day basis, the Director of Finance & Resources has been allocated as the Responsible person for the managing of data protection in school. This individual will have professional experience and knowledge of data protection law, particularly that in relation to schools.

The Director of Finance & Resources will report to the highest level of management at the school, which is the Principal. The Principal acts as the representative of the data controller on a day-to-day basis.

The DPO will operate independently.

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

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.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
 - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
 - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
 - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
 - Reasons of substantial public interest on the basis of 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 Article 89(1).

Consent

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

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

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

The school 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.

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

The right to be informed

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 school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

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

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

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

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

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

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

- Within one month of having obtained the data.

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

Subject Access Requests

We use our DPO for advice and administration of all subject access requests. This includes their best practice approach to redaction and removal of third party data. Third party data is referred to as data which is included in the subject access request but that pertains to individuals who have not given their permission to have their data released. This is particularly (but not exclusively) the case with communications such as emails or child protection information.

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally
- Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:
 - Name of individual
 - Correspondence address
 - Contact number and email address
 - Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the Principal.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from

parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge however, the school 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.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- Where a request is manifestly unfounded or excessive, the school 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 school will ask the individual to specify the information the request is in relation to.
- We may not disclose information for a variety of reasons, such as if it:
 - Might cause serious harm to the physical or mental health of the pupil or another individual
 - Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
 - Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
 - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

It should be noted that the school staff are instructed to delete e-mails at the end of each academic year.

The right to rectification

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

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

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

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

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

The right to erasure

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

Individuals have the right to erasure in the following circumstances:

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

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

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

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

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

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

The right to restrict processing

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school 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 school 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 school has verified the accuracy of the data;
- Where an individual has objected to the processing and the school 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 school 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 school 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 school will inform individuals when a restriction on processing has been lifted.

The right to data portability

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

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

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

- To personal data that an individual has provided to a controller;

- Where the processing is based on the individual's consent or for the performance of a contract;
- When processing is carried out by automated means.

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

The school will provide the information free of charge.

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

Salendine Nook High School 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 school will consider whether providing the information would prejudice the rights of any other individual.

The school 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 school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

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

Individuals have the right to object to the following:

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

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

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

Where personal data is processed for direct marketing purposes:

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

Where personal data is processed for research purposes:

- The individual must have grounds relating to their 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 school 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 school will offer a method for individuals to object online.

Privacy by design and privacy impact assessments

The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school 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 school's data protection obligations and meeting individuals' expectations of privacy.

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

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

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

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

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

The school 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 school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Data breaches

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

The Principal will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training. This will include clarity re possible staff disciplinary actions when staff have failed to comply with the GDPR.

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

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school 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 school 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.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#)

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

The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

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.

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

Data security

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

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

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up 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 will not be used to hold personal information unless they are password-protected and fully encrypted.

All electronic devices are password-protected to protect the information on the device in case of theft.

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

Staff and governors may use their personal laptops or computers for school purposes, but must not store any school/personal data on there.

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.

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 school premises accepts full responsibility for the security of the data.

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
 - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
 - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

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 school containing sensitive information are supervised at all times.

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

Salendine Nook High School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The Director of Finance & Resources is responsible for continuity and recovery measures are in place to ensure the security of protected data.

Publication of information

Salendine Nook High School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures

- Annual reports
- Financial information

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

Salendine Nook High School will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

CCTV and photography

- CCTV can contribute to the security and health and safety of all pupils, staff and visitors.
- The purpose of CCTV at Salendine Nook High School is to provide monitoring systems that assist with the protection of the property, law enforcement, traffic management, community safety and the reduction of crime and disorder, thereby improving the quality of life for all students, staff and visitors to the school.
- The CCTV systems at the Salendine Nook High School have been notified to the Information Commissioner.
- The general management of CCTV at the Salendine Nook High School is currently vested with the Director of Finance & Resources.
- The day to day management of the CCTV system is the responsibility of the ICT Manager.
- Owner Operator Data and Controller of the Scheme – Principal, Salendine Nook High School, New Hey Rd. Huddersfield HD3 4GN.

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

The school notifies all pupils, 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.

Approved list of school staff that have access to CCTV footage is available from the Finance & Admin Teams and is included here as Appendix 1. All other staff must make a request to a member of SLT.

If you require the CCTV to then be copied to disc/pen drive all staff must request this from a member of SLT.

Images are retained on a hard disc for a period of 10 days. Copies can be made for investigation purposes, but requests for copies must be made via the Principal and must be returned, for destruction within 24 days to the Director of Finance & Resources.

All CCTV saved footage for minor incidents will only be kept for a maximum of 28 days. CCTV footage for more serious incidents will be kept for as long as the student's behaviour record is kept,

as this will form part of that record. (see Section 2 above) Once the retention period has expired, the images will be erased.

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

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

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

Remote learning

In certain unusual circumstances, school closure can happen, for example during illness pandemics, during such times the ongoing education of students who cannot be at school, but are able to continue with their education will need a means to support that. This can be facilitated through remote learning.

Any remote working methods will adhere to data protection guidelines.

Accessing personal data

When accessing personal data for remote learning purposes, all staff members will:

- Only access the data on a secure cloud service or a server on the school's IT network
- Ideally staff should only use devices to access data that have been provided by school, such as school-based equipment, rather than using their own personal devices

Processing personal data

Staff members may need to collect and/or share personal data such as part of the remote learning system. As long as this processing is necessary for the school's official functions, individuals won't need to give permission for this to happen.

However, staff are reminded to collect and/or share as little personal data as possible online.

Keeping devices secure

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing antivirus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Data retention

Data will not be kept for no longer than is necessary.

Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the school 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.

e-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards. However, it may be that some e-mails do need to be kept and should therefore be identified by content; for example, if it forms part of a pupil record or a staff /supplier contract. The retention for keeping these e-mails will then correspond with the classes of records according to the content in the retention schedule for schools found in the Records Management Tool Kit for Schools.

These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

If an e-mail is not required to be kept then staff should delete these e-mails within a reasonable timeframe, which would be a maximum of 12 months.

The end of each academic year would be a good time for staff to complete a housekeeping exercise on their kept e-mails, but this may also be done throughout the school year.

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.

Policy review

This policy is reviewed every two years by the Data Protection Officer, Director of Finance & Resources and the Principal.

Appendix 1

Staff Access Rights

Level	Title	Access
1	ICT Technical Team	Full Access and operational use
1	SLT	Full Access and operational use
2	Finance & Admin Team	Downloading, Copying & Viewing of CCTV footage
3	All HoY's, all SSM's & all SSC staff	Viewing access only

ALL other staff will need to make a request to a member of SLT

