GDPR Data Protection Policy

Date Adopted: May 2018

Review Date: September 2024

Next Review: September 2025

Contents:

Statement of intent

Shaw Primary Academy is required to keep and process certain information about its staff members, pupils, their families, volunteers and external contractors in accordance with its legal obligations under data protection legislation.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, DfE, 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 school complies with the following core principles of the UK GDPR.

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

1. [] Legal framework

[] This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- [] DfE (2023) 'Keeping children safe in education 2023'

[] This policy also has regard to the following guidance:

- [] ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- [] DfE (2023) 'Data protection in schools'

This policy operates in conjunction with the following school policies:

- Parental Agreement including use of Photography and Videos
- E-safety Policy
- Publication Scheme
- Child Protection and Safeguarding Policy
- Records Management Policy

2. 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 UK 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, schools are only able to process this if it is either:

- Under the 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 exercising 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.

In accordance with the requirements outlined in the 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 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 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.

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

3. Accountability

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

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 also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

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

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

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

DPIAs will be used to identify and reduce data protection risks, where appropriate.

4. Data protection officer (DPO)

Schools are required to appoint a DPO who will be the central point of contact for all data subjects and others in relation to matters of data protection.

A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws.
- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on DPIAs, conducting internal audits, and providing the required training to staff members.
- Cooperate with the ICO and act as the first point of contact for the ICO and for individuals whose data is being processed.

The DPO is responsible for:

- Coordinating a proactive and preventative approach to data protection.
- Calculating and evaluating the risks associated with the school's data processing.
- Having regard to the nature, scope, context, and purposes of all data processing.
- Prioritising and focussing on more risky activities, e.g. where special category data is being processed.
- Promoting a culture of privacy awareness throughout the school community.
- Carrying out ad hoc reviews of data practices to ensure staff understand and are acting in accordance with relevant data protection laws.

The individual appointed as DPO will have professional experience and be highly knowledgeable about data protection law, particularly that in relation to schools. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

The DPO will operate independently and will not be dismissed or penalised for performing their duties. Sufficient resources and appropriate access will be provided to the DPO to enable them to meet their UK GDPR obligations.

The DPO will report to the highest level of management at the school, which is the governing board.

Staff will ensure that they involve the DPO in all data protection matters closely and in a timely manner.

5. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary 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 school in the performance of its tasks

The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

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 with a basis in 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 with a basis in law
  - 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 a basis in law
- When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

The school has privacy notices for the following groups, which outline the information above that is specific to them:

- Pupils and their families
- School workforce
- Trustees and governors

There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.
- Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met, and the school does not exploit any imbalance of power in the relationship between the school and the child.

6. Consent

Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words 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. Consent can be withdrawn by the individual at any time.

Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

The school ensures that consent mechanisms meet the standards of the UK 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 UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school 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 school on a case-by-case basis, taking into account the requirements outlined above.

7. The right to be informed

Adults and children have the same right to be informed about how the school uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

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, the controller's representative, where applicable, and the DPO
- The purpose of, and the lawful 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, as well as any possible consequences of failing to provide the personal data, will be provided – this information will be supplied at the time the data is obtained.

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

8. The right of access

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and 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 school 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 school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. 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.

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

Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.

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 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.

The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:

- Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
- Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents or it is reasonable to comply without consent.
- Explain to the individual who made the SAR why their request could not be responded to in full.

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 – the time limit for responding to the request will be paused until clarification from the individual is received.

9. The right to rectification

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

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 for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once. The school reserves the right to refuse to process requests for rectification if they are manifestly unfounded or excessive or if exemptions apply.

The school will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

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.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, 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.

10. 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 or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- 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 will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

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 establishment, exercise or defence of legal claims

The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

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.

11. The right to restrict processing

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

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

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 inform individuals when a restriction on processing has been lifted.

Where the school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

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 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 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.

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

- Where personal data has been provided directly by an individual 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 can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

The school will provide the information free of charge.

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.

13. The right to object

The school 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, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- 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.
- The school will respond to objections proportionally, 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 right to object is absolute and 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.
- The school 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 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.

The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The school will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.

Where no action is being taken in response to an objection, 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.

14. Automated decision making and profiling

The school will only ever conduct solely automated decision making with legal or similarly significant effects is the decision is:

- Necessary for entering into or performance of a contract.
- Authorised by law.
- Based on the individual's explicit consent.

Automated decisions will not concern a child nor use special category personal data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest.

The school will conduct a DPIA for automated decision making to mitigate risk of errors, bias and discrimination.

The school will ensure that individuals concerned are given specific information about the processing and an opportunity to challenge or request a review of the decision.

Individuals have the right not to be subject to a decision when both of the following conditions are met:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

The school 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 school 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.

15. Data protection by design and default

The school will act in accordance with the UK GDPR by adopting a data protection by design and default approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into all aspects of processing activities. In line with the data protection by default approach, the school will ensure that only data that is necessary to achieve its specific purpose will be processed.

The school will implement a data protection by design and default approach by using a number of methods, including, but not limited to:

- Considering data protection issues as part of the design and implementation of systems, services and practices.
- Making data protection an essential component of the core functionality of processing systems and services.
- Automatically protecting personal data in school ICT systems.
- Implementing basic technical measures within the school network and ICT systems to ensure data is kept secure.
- Promoting the identity of the DPO as a point of contact.
- Ensuring that documents are written in plain language so individuals can easily understand what is being done with personal data.

16. Data Protection Impact Assessments (DPIAs)

DPIAs will be used in certain circumstances 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 the school's reputation which might otherwise occur. A DPIA will be carried out when using technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, and 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 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 UK GDPR.

17. 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 headteacher will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

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.

Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, and the individuals concerned will be contacted directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. 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 sufficiently serious, the public will be notified without undue delay.

Within a breach notification to the supervisory authority, 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

Where notifying an individual about a breach to their personal data, the school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

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

The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

18. Data security

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

Where possible, staff and governors will not use their personal laptops or computers for school purposes. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

If staff and governors need to use their personal laptops for school purposes, particularly if they are working from home, they will bring their device into school before using it for work to ensure the appropriate software can be downloaded and information encrypted.

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 staff will always check that the recipient is correct before sending.

Before sharing data, all staff 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.

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.

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 on a regular basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.

The school will regularly test, assess and evaluate the effectiveness of any and all measures in place for data security.

The school takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action. The Finance Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

When disposing of data, paper documents will be shredded and digital storage devices will be physically destroyed when they are no longer required. ICT assets will be disposed of in accordance with the ICO's guidance on the disposal of ICT assets.

The school holds the right to take the necessary disciplinary action against a staff member if they believe them to be in breach of the above security measures.

19. Safeguarding

The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.
- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

The school will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the school will seek independent legal advice.

20. Publication of information

The school publishes a Freedom of Information 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 Freedom of Information Publication Scheme are made available quickly and easily on request.

The 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.

21. CCTV and photography

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. All CCTV footage will be kept for 30 days for security purposes; the Finance Manager is responsible for keeping the records secure and allowing access.

Before the school is able to obtain the data of pupils or staff, it is required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

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 or 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. Precautions, as outlined in the Photography and Images Policy, are taken when publishing photographs of pupils, in print, video or on the school website.

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

Parents and others attending school events are able to take photographs and videos of those events as long as they are for domestic purposes only. Photographs or videos being used for any other purpose are prohibited to be taken by parents or visitors to the school.

The school 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.

22. 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, , 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 DPO 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 DPO. The DPO 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 DPO 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 headteacher

23. Data retention

Data will not be kept for 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.

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. Monitoring and review

This policy is reviewed annually by the DPO and the headteacher. The next scheduled review date for this policy is September 2024

26. Appendices

Appendix A

Privacy Notice

Under the UK GDPR and Data Protection Act 2018, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'Privacy Notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This Privacy Notice explains how we collect, store and use personal data about pupils and parents.

Shaw Primary Academy is the 'data controller' for the purposes of Data Protection law.

Our Data Protection Officer is Andy Crow, dpo@dpoforeducation.co.uk

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils, parents and staff includes, but is not restricted to:

Contact details, contact preferences, date of birth, identification documents

Bank account details, payroll records, National Insurance number and tax status information

Results of internal assessments and externally set tests

Pupil and curricular records

Characteristics, such as eligibility for free school meals, or special educational needs

Exclusion information

Attendance information

Safeguarding information

Details of any support received, including care packages, plans and support providers

Photographs

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- Fulfill a contract with you
- Carry out a task in the public interest

Less commonly, we may also process personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)
- We have legitimate interests in processing the data – for example, where:
    - Fraud prevention
    - Ensuring network and information security

Where we have obtained consent to use personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While most of the information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We follow the Information and Records Management Society's Toolkit for schools, click here *Information and Records Management Society's toolkit for schools*

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- The Department for Education - to meet our legal obligations as part of data collections such as the School Census
- Local authorities such as Thurrock Council.
- The pupil's family and representatives – in case of emergencies such as a health matter
- Educators and examining bodies – necessary for the performance of our education function
- Our regulator, Ofsted – to enable it to evaluate the education we provide to your child/ward, which is in the public interest
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Follow on schools/other schools – which your child/ward attends after leaving their current Academy, in the public interest of delivering education
- Our auditors – to meet our finance obligations as part of a statutory requirement ie Annual Report and Accounts
- Health and social welfare organisations/third parties – to enable us to comply with our duty of care and statutory safeguarding duties for your child/ward's welfare. This may include Therapists, Clinical Psychologists, Academy Medical Staff, CAHMS (Child and Adolescent Mental Health Service), School Counsellors, Social Care, Educational Welfare Office (EWO)
- Professional bodies – necessary for the performance of our education function
- Police forces, courts, tribunals – in order to uphold law and order

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally

We may transfer personal data that we collect from you to third-party data processors in countries that are outside the UK. If we do this, we have procedures in place to ensure your data receives the same protection as if it were being processed in the UK. For example, our contracts with third parties stipulate the standards they must follow at all times.

Any transfer of your personal data will follow applicable laws and we will treat the information under the guiding principles of this Privacy Notice.

.

Data Security and Confidentiality

Protecting the confidentiality and integrity of your personal data is a responsibility that we take seriously. We use appropriate technical and organisational measures to keep personal data secure against unauthorised or unlawful processing, and against accidental loss, destruction or damage. For example

- Shaw Academy Trust's employees have received training in Data Protection and how to handle your personal data
- Access to your personal data is restricted to the relevant employees that are required to process your data
- We endeavour to be a paperless school, however if hard copies are created, these are securely stored.
- Your personal data will be periodically reviewed and securely deleted if required
- Internal systems and networks are regularly tested

Photographs and Media

As part of our activities, we may take photographs and allow external organisations to take photographs or to film within our school. You will be made aware when this is happening and the context in which the photograph will be used, and consent will be sought from parents at the start of each school year.

We will take photographs for use by the school. Usually these will be unnamed and will generally be for internal School use but may also include photographs for publications such as:

- Photographs included in the School's Prospectus
- Photographs to be used on display boards which can be seen by visitors to the school
- Photographs posted on the school's official social media sites such as Twitter and its own website. Such sites can be accessed by the public and will therefore require close monitoring by School staff to ensure they are appropriate.

Named photographs will be used for internal use where there is a clear lawful basis for doing so ie, for identifying pupils such as medical or safeguarding requirements.

Parents and pupils' rights regarding personal data

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

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

If you make a subject access request, and if we do hold information about you or your child, we will:

Give you a description of it

Tell you why we are holding and processing it, and how long we will keep it for

Explain where we got it from, if not from you or your child

Tell you who it has been, or will be, shared with

Let you know whether any automated decision-making is being applied to the data, and any consequences of this

Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our Data Protection Officer.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

Object to the use of personal data if it would cause, or is causing, damage or distress

Prevent it being used to send direct marketing

Object to decisions being taken by automated means (by a computer or machine, rather than by a person)

In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing

Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our Data Protection Officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our Data Protection Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

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

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact the school directly or our **Data Protection Officer**:

Andy Crow, dpo@dpoforeducation.co.uk Tel 01702 660234

Appendix B

Subject Access Request Policy and Procedure

1. Scope

All personal data processed within the Shaw Primary Academy is within the scope of this procedure.

For information to be personal data, it must relate to a living individual and allow that individual to be identified from that information (either on its own or in conjunction with other information held alongside it).

The individual to whom the personal data relates to is the 'Data Subject'.

A Subject Access Request (SAR) can be made by

- A pupil of the school
- any parent/carer acting on behalf of their child(ren) as the Data Subject or
- any parent/carer acting in their own individual right as the Data Subject or
- any member of staff as the Data Subject

Data subjects are entitled to obtain:

- Confirmation as to whether Shaw Primary Academy is processing any personal data about that individual;
- Access to their personal data;
- Any related information;
- The logic involved in any automated decisions relating to him or her

2. Responsibilities

2.1 The Data Protection Coordinator is responsible for the application and effective working of this procedure, and for reporting to the information on Subject Access Requests (SARs).
2.2 The Data Protection Coordinator is responsible for handling all SARs.
2.3 The Data Protection Officer advises and signs off the request.

3. Procedure

3.1 Subject Access Requests can be made using the Subject Access Request form, verbally or via email or post
3.2 The data subject provides Shaw Primary Academy with evidence of their identity for example in the form of a current passport/driving licence,
3.3 Where possible, the data subject specifies to Shaw Primary Academy the set of data held by the school on their subject access request (SAR). The data subject can request all data held on them.
3.4 The school records the date that the identification checks were conducted, and the specification of the data sought.
3.5 The school provides the requested information to the data subject within one month from this recorded date.
3.6 Once received, the subject access request (SAR) application is immediately forwarded to the Data Protection Coordinator, and or the DPO, who will ensure that the requested data is collected within the specified time frame in clause 3.4 above.
Collection entails:

3.6.1 Collecting the data specified by the data subject, or
3.6.2 Searching all databases and all relevant filing systems (manual files) within the school, including all back up and archived files (computerised or manual) and all email folders and archives. The Data Protection Coordinator maintains a data map that identifies where all data in each school is stored.

3.7 The Data Protection Coordinator maintains a record of requests for data and of its receipt, including dates. This is shared with the DPO.

3.8 The Data Protection Coordinator reviews subject access requests from a child. Before responding to a SAR of the child, the Data Protection Coordinator considers their ability to making the request.

3.9 The Data Protection Coordinator reviews all documents that have been provided to identify whether any third parties are present in it, and either removes the identifying third party information from the documentation or obtains written consent from the third party for their identity to be revealed.

3.10 Some of the data being processed may be exempt from being included in a Subject Access Request under the Data Protection Act 2018 and would have to be checked before being included.

3.11 In the event that a data subject requests Shaw Primary Academy to provide them with the personal data stored by the controller/processor, then the school will provide the data subject with the requested information in electronic format, unless otherwise specified. All of the items provided to the data subject are listed in a schedule that shows the data subject's name and the date on which the information is delivered to the data subject.

3.12 In the event that a data subject requests what personal data is being processed then the school provides the data subject with the following information:

- 3.12.1 Purpose of the processing
- 3.12.2 Categories of personal data
- 3.12.3 Recipient(s) of the information, including recipients in third countries or international organisations
- 3.12.4 How long the personal data will be stored
- 3.12.5 The data subject's right to request rectification or erasure, restriction or objection, relative to their personal data being processed.
  - 3.12.5.1 Shaw Primary Academy removes personal data from systems and processing operations as soon as a request for erasure has been submitted by the data subject.
  - 3.12.5.2 Shaw Primary Academy contacts and communicates with other organisations, where the personal data of the data subject is being processed, to cease processing information at the request of the data subject.
  - 3.12.5.3 Shaw Primary Academy takes appropriate measures without undue delay in the event that the data subject has withdrawn consent, objects to the processing of their personal data in whole or part no longer under legal obligation and/or has been unlawfully processed.
- 3.12.6 Inform the data subject of their right to lodge a complaint with the supervisory authority and a method to do so (Complaints Procedure).
- 3.12.7 Information on the source of the personal data if it hasn't been collected from the data subject.

3.12.8 Inform the data subject of any automated decision-making.
3.12.9 If and where personal data has been transferred and information on any safeguards in place.

4. Document Owner and Approval

The Data Protection Coordinator and the Data Protection Officer are the owners of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the DPA2018 & UK GDPR.

Appendix C

Data Processing Agreement

This agreement is made effective from day of 20xx between the undersigned parties:

I. Shaw Primary Academy *(Controller of the data)* whose trading address is at Avon Grn, South Ockendon RM15 5QJ
II. XXX Ltd (Processor of data) whose trading address is xxx

1. Terms of Agreement

1.1 This agreement supplements the Principal Contract and makes legally binding provisions for compliance with the Data Protection Laws as set forth in this agreement. As per the requirements of relevant Data Protection Law, all processing of personal data by a processor on behalf of a controller, shall be governed by a contract.

1.2 The terms used in this agreement have the meanings as set out in the *'definitions'* part of the document

2. Obligations and Rights of the Processor

2.1 The Processor shall comply with the relevant Data Protection Laws and must: -

a) only act on the written instructions of the Controller
b) ensure that people processing the data are subject to a duty of confidence
c) ensure that any natural person acting under their authority who has access to personal data, does not process that data except on instructions from the Controller

d) use its best endeavours to safeguard and protect all personal data from unauthorised or unlawful processing, including (but not limited to) accidental loss, destruction or damage and will ensure the security of processing through the demonstration and implementation of appropriate technical and organisational measures required by the UK GDPR
e) ensure that all processing meets the requirements of the UK GDPR and Data Protection Act 2018 and is in accordance with the Data Protection Principles
f) ensure that where a Sub-Processor is used, they: -
    i. only engage a Sub-Processor with the prior consent of the data controller
    ii. inform the controller of any intended changes concerning the addition or replacement of Sub-Processors
    iii. they implement a written contract containing the same data protection obligations as set out in this agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Protection Laws
    iv. understand that where any Sub-Processor is used on their behalf, that any failure on the part of the sub-processor to comply with the Data Protection Laws or the relevant data processing agreement, the initial processor remains fully liable to the controller for the performance of the Sub-Processor's obligations
g) assist the Controller in providing subject access and allowing data subjects to exercise their rights under the Data Protection Laws
h) assist the Controller in meeting its data protection obligations in relation to: -
i) the security of processing
j) data protection impact assessments
k) the investigation and notification of personal data breaches
l) delete or return all personal data to the Controller as requested at the end of the contract
m) make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the relevant Data Protection Laws and allow for, and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller
n) tell the Controller immediately if they have done something (or are asked to do something) infringing the UK GDPR
o) co-operate with supervisory authorities in accordance with UK GDPR Article 31
p) notify the Controller of any personal data breaches in accordance with UK GDPR Article 33
q) where applicable, employ a Data Protection Officer if required

2.2 Nothing within this agreement relieves the processor of their own direct responsibilities, obligations and liabilities under the UK GDPR or other Data Protection Laws.

2.3 The Processor is responsible for ensuring that each of its employees, agents, subcontractors or vendors are made aware of its obligations regarding the security and protection of the personal data and the terms set out in this agreement.

2.4 The Processor shall maintain induction and training programs that adequately reflect the Data Protection Law requirements and regulations, and ensure that all employees are afforded the time, resources and budget to undertake such training on a regular basis.

2.5 Any transfers of personal data to a third country or an international organisation shall only be carried out on documented instructions from the controller; unless required to do so by Union or Member State law. Where such a legal requirement exists, the Processor shall inform the Controller of that legal requirement before processing.

2.6 The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing: -

a) the name and contact details of the Processor and of each Controller on behalf of which the Processor is acting, and, where applicable, the data protection officer
b) the categories of processing carried out on behalf of each Controller
c) transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards
d) a general description of the technical and organisational security measures referred to in Article 32(1)

2.7 The Processor shall maintain records of processing activities in writing, including in electronic form and shall make the record available to the supervisory authority on request.

2.8 When assessing the appropriate level of security and the subsequent technical and operational measures, the processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Obligations and Rights of the Controller

1.1. The Controller is responsible for verifying the validity and suitability of the Processor before entering into a business relationship.

1.2. The Controller shall carry out adequate and appropriate onboarding and due diligence checks for all Processors, with a full assessment of the mandatory Data Protection Law requirements.

1.3. The Controller shall verify that the Processor has adequate and documented processes for data breaches, data retention and data transfers in place.

1.4. The Controller shall obtain evidence from the Processor as to the: -

a) verification and reliability of the employees used by the Processor
b) certificates, accreditations and policies as referred to in the [due diligence/onboarding questionnaire]
c) technical and operational measures
d) procedures in place for allowing data subjects to exercise their rights, including (but not limited to), subject access requests, erasure & rectification procedures and restriction of processing measures

1.5. Where the Controller has authorised the use of any Sub-Processor by the initial Processor, the controller must verify that similar data protection agreements are in place between the initial Processor and Sub-Processor.

4. Penalties & Termination

4.1 By signing this agreement, the Processor confirms that they understand the legal and enforcement actions that they may be subject to should they fail to uphold the agreement terms or breach the Data Protection Laws. If the processor fails to meet their obligations, they may be subject to: -

a) investigative and corrective powers of supervisory authorities under the UK GDPR
b) an administrative fine under the UK GDPR
c) a penalty under the UK GDPR
d) pay compensation under the UK GDPR

4.2 The Controller or Processor can terminate this agreement with immediate effect.

5. Definitions

In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings: -

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

Data Protection Laws means all applicable Data Protection Laws, including the General Data Protection Regulation (UK GDPR) (EU 2016/679), Data Protection Act 2018 and, to the extent applicable, the data protection or privacy laws of any other country

EEA means the European Economic Area

Effective Date means that date that this agreement comes into force

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

UK GDPR means the General Data Protection Regulation (UK GDPR) (EU) (2016/679)

Principal Contract means the main contract between the parties named in this agreement

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

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of this data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing

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

Sub Processor means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller

Signed on behalf of the Processor:

IN WITNESS below of the parties or their duly authorised representatives have signed this agreement in accordance with all its clauses and on the day, month and year stated at the top of this agreement.

Signed:

Print Name:

Date:

Company Name:

Position:

Signed on behalf of the Controller:

Signed:

Print Name:

Date:

Appendix D

Data Breach Policy and Procedure

1. Introduction

This document sets out the guidance and procedure for personal data breach incidents and must be read in conjunction with the School's Data Protection Policy.

2. Purpose and Scope

The purpose of this procedure is to provide a framework within which Shaw Primary Academy will ensure compliance with the legislative requirements of managing a personal data breach incident or suspected personal data breach incident.

This procedure applies to school staff, agency workers, volunteers, contractors and third party agents who process data for or on behalf of the school and it must be complied with in the event of a personal data breach.

The school is required to keep a record of all security incidents involving personal data. Some of these incidents must be reported to the Information Commissioner within 72 hours of detection, and without undue delay to individuals affected by the incident. It is vital that all staff report a personal data breach, or suspected personal data breach, however minor, as soon as possible after discovery so that we can use the 72 hours to establish what has happened, the size of the breach and whether it needs to be reported further.

3. Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access to personal data.

4. Examples of a Data Breach

- Loss or theft of personal data or equipment (encrypted and non-encrypted devices) on which personal data is stored, e.g. loss of paper record, laptop, iPad or USB stick
- Inappropriate access controls allowing unauthorised use, e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to personal data or information systems
- Equipment failure
- Human error, e.g. email containing personal data sent to the incorrect recipient
- Unauthorised disclosure of sensitive or confidential information, e.g. document posted to an incorrect address or addressee
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Phishing attacks where information is obtained by deceiving the organisation who holds it

- Insecure disposal of paperwork containing personal data

5. Why should Data breaches be reported?

The longer any incidents go unreported, the harder it gets to resolve any vulnerabilities. Impacted data subjects have a right to know that their data may have been compromised and that they could then take steps that could minimise an adverse impact on them such as informing their bank that their bank details have been compromised.

The longer an incident goes unreported, the longer a vulnerability may remain unaddressed allowing the incident to escalate or for further incidents to occur. Without timely visibility of the incident through reporting the school may not be able to fulfil its legal obligations.

The UK GDPR places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach.
Knowing that a breach has occurred, and delaying reporting reduces the time available for the investigation team to understand and assist with a response and still meet privacy compliance requirements.

Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust to prevent future breaches and protect personal data.

1. **Procedure for reporting a Data Breach**

The primary point of contact for reporting a data breach incident is the School's Data Protection Coordinator and/or the Data Protection Officer (DPO).

Responsibility for reporting a suspected breach lies with the person who discovered the breach. Suspected personal data breach incidents should be reported immediately upon discovery, in writing (or by phone if that is not possible), using the form Incident Report Form supplied on the website or via the office. This form should be sent by email and copied to your line manager (unless there is a need to report it confidentially to the DPO).

The Data Protection Coordinator will investigate the breach and, where appropriate, notify the DPO, the relevant line management and HR.

2. **Breach Reporting to the Information Commissioner's office (ICO)**

The DPO (or nominated deputy) will notify the ICO, without undue delay, of a reportable personal data breach.

3. **Breach Notification- Data Subject**

Where the personal data breach, or suspected personal data breach, is likely to result in impacting the rights and freedoms of the data subject the school shall notify the affected data subjects, without undue delay, in accordance with the DPO's recommendations.

4. **Breach Notification – Third Party**

Where the personal data breach, or suspected personal data breach, is likely to result in impacting the rights and freedoms of the data subject the school shall notify the affected third parties (e.g. joint data controller/ to the controller where School is the processor) without undue delay, in accordance with the DPO's recommendations.
The school may also need to notify others, e.g. the Police and insurers.

5. **Enforcement**

Failure to adhere to this procedure, delay in reporting the breach to the DPO and non-reporting of breaches, may result in disciplinary action in accordance with the school's Staff Disciplinary Procedure.

Appendix D

Data Breach Policy and Procedure

1. Introduction

This document sets out the guidance and procedure for personal data breach incidents and must be read in conjunction with the School's Data Protection Policy.

2. Purpose and Scope

The purpose of this procedure is to provide a framework within which Shaw Primary Academy will ensure compliance with the legislative requirements of managing a personal data breach incident or suspected personal data breach incident.

This procedure applies to school staff, agency workers, volunteers, contractors and third party agents who process data for or on behalf of the school and it must be complied with in the event of a personal data breach.

The school is required to keep a record of all security incidents involving personal data. Some of these incidents must be reported to the Information Commissioner within 72 hours of detection, and without undue delay to individuals affected by the incident. It is vital that all staff report a personal data breach, or suspected personal data breach, however minor, as soon as possible after discovery so that we can use the 72 hours to establish what has happened, the size of the breach and whether it needs to be reported further.

3. Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access to personal data.

4. Examples of a Data Breach

- Loss or theft of personal data or equipment (encrypted and non-encrypted devices) on which personal data is stored, e.g. loss of paper record, laptop, iPad or USB stick
- Inappropriate access controls allowing unauthorised use, e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to personal data or information systems
- Equipment failure
- Human error, e.g. email containing personal data sent to the incorrect recipient
- Unauthorised disclosure of sensitive or confidential information, e.g. document posted to an incorrect address or addressee
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Phishing attacks where information is obtained by deceiving the organisation who holds it
- Insecure disposal of paperwork containing personal data

5. Why should Data breaches be reported?

The longer any incidents go unreported, the harder it gets to resolve any vulnerabilities. Impacted data subjects have a right to know that their data may have been compromised and that they could then take steps that could minimise an adverse impact on them such as informing their bank that their bank details have been compromised.

The longer an incident goes unreported, the longer a vulnerability may remain unaddressed allowing the incident to escalate or for further incidents to occur. Without timely visibility of the incident through reporting the school may not be able to fulfil its legal obligations.

DPO Contact Details:

Email - andy@dpoforeducation.co.uk

Tel - 01702 660234

Appendix E

CCTV Policy

1. Policy Statement

Shaw Primary Academy uses Close Circuit Television (“CCTV”) within its premises. The purpose of this policy is to set out the position of the school as to the management, operation and use of the CCTV at each of its schools.

This policy applies to all members of staff, pupils, local committee members, contractors, visitors to Shaw Primary Academy premises and all other people whose images may be captured by the CCTV system.

Images may also be taken on cameras placed inside school buses.

This policy takes account of all applicable legislation and guidance, including:

- The UK General Data Protection Regulation (“UKGDPR”)
- The Data Protection Act 2018
- CCTV Code of Practice produced by the Information Commissioner
- Human Rights Act 1998

This policy sets out the position of the school in relation to its use of CCTV.

2. Purposes of CCTV

CCTV has been installed by the school with the primary purpose of reducing the threat of crime generally, protecting our premises and helping to ensure the safety of all our staff, pupils and visitors and respect for the individuals’ privacy.

- To provide a safe and secure environment for pupils, staff and visitors
- To deter those with criminal intent and protect the school buildings and/or assets
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders
- To assist in managing the school
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is or is threatened to be taken.

The system will not be used:

- To provide recorded images for the internet
- For any automated decision making

Although every effort has been made to ensure maximum effectiveness of the system, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

3. Description of System

Shaw Primary Academy uses fixed cameras on sites. Cameras are not equipped for sound recording.

4. Siting of Cameras

All CCTV cameras will be positioned in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. Shaw Primary Academy will make all reasonable efforts to ensure that areas outside of the school premises are not recorded.

Signs have been erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

5. Privacy Impact Assessment

Prior to the installation of any new CCTV camera, or system, a privacy impact assessment was conducted by Shaw Primary Academy to ensure that the proposed installation is compliant with legislation and ICO guidance.

Shaw Primary Academy will adopt a privacy by design approach when installing new cameras and systems, considering the purpose of each camera to avoid recording and storing excessive amounts of personal data.

6. Management and Access

The CCTV system will be managed by the Headteacher, Deputy Headteacher and Finance Manager.

On a day to day basis the CCTV system will be operated by staff in the school with delegated authority as appropriate.

The viewing of live CCTV images will be restricted to members of staff in school offices with explicit powers to view images, for the reasons set out above.

Recorded images which are stored by the CCTV system will be restricted to access by members of staff in the school with explicit powers to view images, for the reasons set out above.

No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

The CCTV system is checked and logged half-termly by appropriate staff members in the school to ensure that it is operating effectively. CCTV footage will always be viewed by at least two members of authorised staff.

7. Storage and Retention of Images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

Recorded images are stored only for a period of 30 days unless there is a specific purpose for which they are retained for a longer period.

Shaw Primary Academy will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being in restricted access areas;
- The CCTV system being encrypted/password protected;
- Restriction of the ability to make copies to specified members of staff

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the school.

8. Disclosure of Images to Data Subjects

Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection law and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a Subject Access Request pursuant to the Data Protection law. Such a request should be considered in the context of the school's Subject Access Request Policy.

When such a request is made an appropriate person from the school and at least one other person will review the CCTV footage for the relevant time periods, in accordance with the request.

If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which only contains images of the individual making the request or their child. The school will take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals, then Shaw Primary Academy will consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record will be kept and held securely, of all disclosures which sets out:

- When the request was made;

- The process followed by the appropriate person in determining whether the images contained third parties;

- The considerations as to whether to allow access to those images;

- The individuals that were permitted to view the images and when; and

- Whether a copy of the images was provided, and if so to whom, when and in what format.

9. Disclosure of Images to Third Parties

Shaw Primary Academy will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection law.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received from a law enforcement agency for disclosure of CCTV images the appropriate person in the school must follow the same process as above in relation to Subject Access Requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any

individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10. Review of Policy and CCTV System

The CCTV system and the privacy impact assessment relating to it will be reviewed bi-annually.

11. Misuse of CCTV Systems

The misuse of the CCTV system could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

12. Complaints Relating to this Policy

Any complaints relating to this policy or to the CCTV system operated by the school should be made in accordance with Shaw Primary Academy Complaints Policy

Appendix F

Data Protection Impact Assessment Procedure

1. Scope

All projects that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a Data Protection Impact Assessment (DPIA).

2. Procedure

a. All new processes or technologies that are to be introduced by the organisation are to be assessed by the DPO to ascertain whether or not a DPIA is necessary.

b. The organisation appoints an appropriate member of staff to conduct the DPIA with guidance from the Data protection Coordinator using the form below.

c. The DPIA is submitted to the Data Protection Officer for comment and sign off

d. The Data Protection Coordinator is responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

e. The DPIA is passed to the Governors for final sign off.

f. The organisation is responsible for implementing any privacy risk solutions identified.

Data Protection Impact Assessment Template

Data protection impact assessments must be completed for any new data processing within the school.

Once completed these should be sent to the data protection lead for review who will then pass to the Data Protection Officer for approval.

Step 1: identify the need for a DPIA

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

Step 2: describe the data processing in more detail	
Nature of the data processing	
• *How will you collect, use, store and delete the data?* • *What is the source of the data?* • *Will you be sharing the data with anyone? (You might find it useful to create to a flow diagram)* • *What types of processing are involved that can be identified as potentially high risk?*	
Scope	
• *What is the nature of the data, and does it include special category or*	

criminal offence data? • *How much data will you be collecting and using?* • *How often?* • *How long will you keep it?* • *How many individuals are affected?*	
Context	
• *What is the nature of your relationship with the individuals?* • *Do they include children or other vulnerable groups?* • *How much control will they have over the processing?* • *Would they expect you to use their data in this way?* • *Have there been prior concerns or previous security flaws to do with this type of processing?* • *Is it novel in any way?* • *What is the current state of technology in this area and are there any current issues of public*	

concern that you should factor in?	
Purposes	
• *What do you want to achieve?* • *What is the intended effect on individuals?* • *What are the benefits of the processing for you, and more broadly?*	

Step 3: consultation process	
Explain how you will consult with relevant stakeholders	
• *When and how will you seek individuals' views on your data processing activity?* • *If you feel it's not appropriate to consult with relevant stakeholders, how can you justify this decision? (Make sure you always record any decision not to consult)* • *If you are consulting, who else within your organisation do you need to involve?*	

• *Do you need any of your data processors or any other third parties to help with the consultation?* • *Do you plan to consult information security experts, or any other experts?*	

Step 4: assess necessity and proportionality	
Describe how you will make sure you comply with data protection law, and keep the processing proportionate to what you actually need	
• *What is your lawful basis for processing the data in this way?* • *Does the processing actually achieve your purpose?* • *Is there a less intrusive way to achieve the same outcome?* • *How will you ensure the data is good quality and limited to what is necessary?* • *What information will you give individuals about how their data is used?* • *How will you help to support their rights*	

under the GDPR? • *What measures do you take to ensure processors and other third parties comply with data protection law?* • *How do you safeguard any international transfers of the data?*	

Step 5: identify and assess risks			
Describe the source of risk and the nature of potential impact on individuals *Risks may include:* • *A privacy breach caused by technical issues or human error, where individuals are at risk of discrimination, identity theft, fraud, loss of confidentiality, physical or emotional harm* • *Poor processes or inadequate due diligence leading to non-compliance with the GDPR, resulting in financial or reputational damage to the school*			

Step 6: identify measures to reduce risk				
For risks identified as medium or high, identify additional measures you will take to reduce or eliminate the risk				
Risk	**Options to reduce or eliminate risk**	**Effect on risk *(eliminated, reduced or accepted)***	**Residual risk *(low, medium or high)***	**Measure approved *(yes or no)***

Step 7: sign off and record outcomes		
	Name and date	**Actions**
Completed by:		
Measures approved by:		
Residual risks approved by:		
Submitted to Board:		
Board approved (CEO):		
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:		
If the advice was overruled, explain why:		
If overruled, Board approved:		
Consultation responses reviewed by:		
If your decision is not the same as individuals' views, explain why, and why you have decided to continue with the processing:		

This DPIA will be kept under review by (name):	
Date:	