



Squirrel Hayes First School

Policy Reviewed on	May 2018	May 2019	March 2020	March 2021	March 2022	March 2023	March 2024	December 2024
Policy Owner Signature	SE & KC	SE	SE	SE	SE	SE	NR	NR
Policy adopted by the Governing Body on	May 2018	May 2019	March 2020	March 2021	March 2022	March 2023		
Policy Reviewed Date	May 2019	May 2020	March 2021	March 2022	March 2023	March 2024		
Version	01	02	03	04	05	06	07	08

Data Protection Policy

Contents:

Statement of Intent

Squirrel Hayes First School is required to keep and process certain information about its staff members and learners in accordance with its legal obligations under the GDPR.

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

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

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

This policy complies with the requirements set out in the GDPR, which will come into effect on 25th May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Legal Framework

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

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The School Standards and Framework Act 1998.
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy will also have regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

General Data Protection Regulation (GDPR)

We are committed to ensuring that personal information is properly managed and that we ensure compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). We are committed to making every effort to meet our obligations under the GDPR legislation and will regularly review policies and procedures to ensure that we are doing so. We recognise that each and every employee has a responsibility to comply with the appropriate data protection laws.

Our school and employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of all members of the school to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- Have permission to access that data
- Need to have access to that data

Data breaches can have serious effects on individuals and/or the school concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office (ICO). Particularly, all transfer of data is subject to risk of loss or contamination. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

The GDPR lays down a set of rules for processing of personal data (both structured manual records and digital records). The GDPR:

- Defines what is meant by 'personal data'
- Confers rights on 'data subjects'
- Places obligations on 'data controllers' and 'data processors'
- Creates principles relating to the processing of personal data
- It provides for penalties for failure to comply with the above

Personal Data

Under the GDPR, personal data is defined as: *"Any information relating to an identified or identifiable natural person (data subject); an identifiable 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."*

The Six Principles of the GDPR

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

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

Responsibilities

Article 5(2) of the GDPR requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles." The Governors have overall responsibility for our

compliance with the GDPR and have appointed a Data Protection Officer (DPO) to ensure compliance. The Headteacher is responsible for ensuring compliance with the GDPR and this policy within the day to day activities of the school. The Data Protection Officer (DPO) will support the Headteacher in order to ensure that appropriate training is provided for all staff. Staff need to be aware of their obligations relating to any personal data they process as part of their duties. Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to disciplinary action and potentially criminal prosecution. Everyone has the responsibility of handling personal and sensitive personal data in a safe and secure manner. The school will hold the minimum personal data necessary to enable them to perform their function and will not hold data for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Data Controller

As a data controller, we pay the appropriate Data Protection Fee to the Information Commissioner's Office on an annual basis and also provides contact details for our Data Protection Officer. The ICO publishes a register of fee paying organisations which can be checked online by visiting: <https://ico.org.uk/esdwebpages/search>.

Information Asset Owners (IAO)

The school has identified Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil information, staff information, assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- What information is held, for how long and for what purpose
- How information has been amended or added to over time
- Who has access to protected data and why

Data Protection Officer (DPO)

The GDPR makes it a requirement for public authorities to appoint a Data Protection Officer (DPO). Article 39 of the GDPR defines the minimum tasks of the DPO as follows:

- To inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed

The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools. The DPO will operate independently reporting to the Headteacher and will not be dismissed or penalised for performing their task and duties. The school will ensure that sufficient resources are provided to the DPO to enable them to meet their obligations.

Accountability

Squirrel Hayes First School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. We will provide comprehensive, clear and transparent privacy policies. 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

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

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

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

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Continuously creating and improving security features
- Use of data protection impact assessments, where appropriate

Personal Data

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier (such as IP address).

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised e.g. key-coded can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data

The GDPR has extended the definition of 'sensitive personal data' which requires even more protection than 'personal data'. Sensitive personal data includes data relating to the following:

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

The school and its employees must be careful when handling sensitive personal data, especially if it is necessary to share it with other organisations, to ensure it is adequately protected at all times.

Lawful Processing

Under the GDPR, before any personal data is processed, the data controller has to identify what legal basis they are using to process the data. Data will be lawfully processed under the following conditions:

- The Consent of the data subject has been obtained
- Processing is necessary for:
 - Compliance with legal obligation
 - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
 - For the performance of a contract with the data subject or to take steps to enter a contract
 - Protecting the vital interests of a data subject or another person
 - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject (This condition is not available to processing undertaken by the school in the performance of its tasks)

If processing sensitive personal data, Article 9 of the GDPR sets out further legal bases that a data controller must consider and record before processing takes place:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
 - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
 - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
 - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
 - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
 - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
 - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

The majority of processing carried out by the school will be necessary for the performance of a task carried out in the public interest. As a public authority, it is in the public interest that the school educates our children. Accordingly, for all the common tasks carried out by the school we do not need to ask for the data subject's consent but rather we can use public interest as our legal basis for processing the appropriate personal data.

This legal basis covers our use of personal data for all the everyday tasks within our schools such as:

- Operating a curriculum
- Storing personal data about our pupils including their parental contacts
- Storing personal data about our staff
- Timetable information
- Cashless catering
- The census requirements

However, there could well be some situations where the school might need to obtain explicit consent to process personal data or, at the very least, consider whether consent is needed. These could include situations where we share personal data with third party suppliers. If these are for everyday functions of the school that would be expected by any reasonable person, then 'public interest' may cover this processing. If, on the other hand, the third party supplier is providing a service that might not be expected to be part of everyday school life, then explicit consent would be necessary.

Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. The school will only accept consent where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given. With regards to consent, please note:

- The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease
- Consent previously accepted under the Data Protection Act (DPA) will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained
- Consent can be withdrawn by the individual at any time
- Where a child is under the age of 16, the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child

Individuals Rights

Data subjects (the living individual) that the personal data being processed relates to have the following rights:

- The right to be informed. This means that individuals must be told what data we are using, why and for what purpose
- The right of access. Individuals have to be allowed to see what data of theirs we are processing if they request it
- The right of rectification. If data is wrong, we have to correct it

- The right to erasure. Individuals can demand that all data of theirs be erased unless we have a legitimate legal basis for continuing to do so
- The right to restrict processing. Individuals can demand that we stop using their data unless we have a legitimate legal basis for continuing to do so
- The right to data portability. Individuals can decide to move their data to another processor and we have to provide them with all their data so they can do this, however, this only applies to data processed by automated means
- The right to object. Individuals can object to our use of their data and we must stop using it unless we have an overriding legitimate reason to continue
- Rights in relation to automated decision making or profiling. Individuals can demand that automated decisions about them are reviewed by a human.

The Right to be Informed (Privacy Notice)

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

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

- The identity and contact details of the controller and the DPO
- The purpose of, and the legal basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place
- The retention period or criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
 - Withdraw consent at any time
 - To lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences
- Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided
- Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

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

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

Information to Pupils and their Families – the “Privacy Notice”

In order to comply with our data protection obligations, we will inform pupils and parents/carers of all pupils of the data we collect, process and hold, the purposes for which the data is held, our legal basis for doing so, how long we will keep the data for and the third parties such as the

Local Authority and Department for Education to whom it may be passed. This privacy notice will be passed to pupils and parents/carers through a specific letter. Parents/carers of new Pupils to our schools will be provided with the privacy notice as part of the admissions process. Our privacy notices can be found in **Appendix A** and on our website.

Information to the Workforce – the “Privacy Notice”

In order to comply with our data protection obligations, we will inform all staff of the data we collect, process and hold about them, the purposes for which the data is held, our legal basis for doing so, how long we will keep the data for and the third parties such as the Local Authority, Department for Education and HMRC to whom it may be passed. This privacy notice will be passed to staff through a specific letter. New staff joining our school will be provided with the privacy notice as part of their induction process. Our Workforce privacy notice can also be found in **Appendix B** and on our website.

The Right of Access (Data Subject Access Requests)

Individuals have the right to obtain confirmation that their data is being processed. Individuals also have the right to submit a Data Subject Access Request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing. A DSAR will provide the data subject with:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

When responding to a DSAR:

- We will verify the identity of the person making the request before any information is supplied by asking for two forms of identification
- We may also contact the individual via phone to confirm the request was made
- A copy of the information will be supplied to the individual free of charge; however, a 'reasonable fee' may be imposed to comply with requests for further copies of the same information
- Where a DSAR has been made electronically, the information will be provided in a commonly used electronic format
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged
- All fees will be based on the administrative cost of providing the information
- All requests will be responded to without delay and at the latest, within one month of receipt
- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request
- 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

- 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 judicial remedy, within one month of the refusal.

When responding to a DSAR we will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

Data Subject Access Requests must be submitted in writing, either by letter or email to the DPO. They should include:

- The name of the individual
- The correspondence address
- A contact number and email address
- Details of the information requested

If staff receive a DSAR they must immediately forward it to the DPO.

Children and Data Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils below the age of 12 may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

The Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, we will inform them of the rectification where possible. Where appropriate, we will inform the individual about the third parties that the data has been disclosed to. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, we will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing

- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

We have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

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

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The Right to Restrict Processing

Individuals have the right to block or suppress the school's processing of personal data. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

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

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

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

The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability.

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

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

Personal data will be provided in a structured, commonly used and machine-readable form free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. We are not required to adopt or maintain processing systems which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual. We 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, we will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The Right to Object

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

Individuals have the right to object to the following:

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

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

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

Where personal data is processed for direct marketing purposes:

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

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object
- Where the processing of personal data is necessary for the performance of a public interest task, the school are 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.

Automated Decision Making and Profiling

Individuals have the right not to be subject to a decision when:

- 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, we will ensure that the appropriate safeguards are in place, including:

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

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

- The school have the explicit consent of the individual
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

Data Protection Impact Assessments (DPIAs)

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

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used for more than one project, where necessary.

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

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

The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes

- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

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

Where it is unclear whether a DPIA is required, the school will refer to the following screening questions provided by Staffordshire County Council:

1. Will the project involve the collection of new information about individuals?
2. Will the project compel individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for or in a way it is not currently used?
5. Does the project involve you using new technology which might be perceived as being privacy intrusive? E.g. Use of biometrics or facial recognition?
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. Health records, criminal records or other information that people would consider particularly private?
8. Will the project require you to contact individuals in ways which they may find intrusive?

If the answer to any of the screening questions is Yes, then a DPIA will need to be completed.

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 and Senior Leadership Team will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training. All staff members must ensure that suspected breaches are reported to the Headteacher or a member of the schools Data Governance Team immediately.

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

All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, the public will be notified without undue delay. Effective and robust breach detection, investigation and internal reporting procedures are in place across the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

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

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

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

Working from home & Security and Remote Access

An effective bring your own device policy can lead to a number of benefits including improved increased job efficiency and increased flexibility. Careful assessment and management of risks to data protection at the outset, embeds data protection at the core of its business activities and to raise overall standards.

Personal device security: laptops and tablets

Due to the portability of personal devices and risk of loss or theft, every effort should be made to ensure that the data is secure.

- Strong passwords to secure your devices will be changed regularly
- Laptops must be encrypted
- Laptop should have automatic locks if inactive for a period
- There must be a clear separation between the personal data processed on behalf of the data controller and that processed for the laptop owner's own purposes E.G. using different apps for business and personal use
- Anti-virus software is regularly updated
- Individual users have separate accounts
- Privacy screen filters are to be used
- Data is accessed in secure areas
- The laptop is locked if left unattended
- Laptops are used in secure areas
- Users are aware about the risks to downloading untrusted or unverified apps

- Users are accountable for the safe and secure deletion of the data throughout the lifecycle of the device, and particularly if the device is to be sold or transferred to a third-party or when leaving employment.
- USB flash drives to store or transfer data are encrypted
- All personal data should be anonymised as far as practicable
- Data should only be stored for required period of time

Types of data that can be stored on a personal device

- Unclassified - documents with not personal data that can be shared publically
- Personal - this should be anonymised

Types of data that require additional confidential storage

- Official - sensitive restricted data may not be stored on personal devices and should be stored securely in the cloud.

Mobile phones for emails

- Mobile phones and tables are pin protected
- All mobile phones are always safe and secure
- Personal data is never sent through accounts not supplied by school
- Information through reply to ensure that it reaches the correct recipient
- If a mobile phone is lost it must be reported as a data breach and where possible the contract provider contacted to reset factory settings or to deactivate the device
- Users are accountable for the safe and secure deletion of the email account and associated data throughout the lifecycle of the device, and particularly if the device is to be sold or transferred to a third-party, or when leaving employment

Software as Service Cloud Storage

Cloud computing services offers a range of benefits such as increased security.

Cloud storage security

- Data may only be stored in cloud storage provided by the school
- Passwords must strong and changed regularly
- Shared access to cloud storage will be limited to level of professional security access
- Users will pay careful attention to read and edit permissions when sharing access

Types of data that can be stored in the cloud

- Unclassified
- Official (Personal)
- Official (Sensitive)

.Paper Records

Paper records provide essential information for some purposes. It may be necessary for paper records to be utilised or updated at home. Paper records present a security risk due to ease of accessibility. Careful assessment and management of risk should be taken when transferring, storing and working with paper records.

Security of Paper Records

- Paper records should not be visible when being transferred between work and home
- Paper records should be stored securely when be transferred or stored
- Paper records are in used discreetly in secure areas

Security

Security is paramount to all data processing throughout Squirrel Hayes First and all staff are required to ensure that all personal/sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period:

- Paper records containing personal/sensitive information must not be left unattended or in clear view anywhere with general access
- Paper records containing personal/sensitive information must be kept in a locked filing cabinet, drawer or safe, with restricted access
- Any personal/sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day
- Filing cabinets containing personal/sensitive information must be kept closed and locked when not in use or when not attended
- Keys used for access to personal/sensitive information must not be left at an unattended desk
- Computer workstations must be locked when workspace is unoccupied
- Computer workstations must be shut completely down at the end of the work day
- Digital data stored on local hard drives and network drives are backed up daily to the server.
- Memory sticks must not be used to hold personal information unless they are password-protected and fully encrypted. Data from our systems will only be saved to school encrypted USB memory sticks; any data used and saved outside of school, on encrypted memory sticks should be backed up in school as soon as possible.
- All necessary members of staff are provided with their own secure login and passwords.
- Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location
- Internal emails containing sensitive or confidential information are password-protected
- External emails containing sensitive or confidential information are sent via encrypted email
- Circular emails, (i.e. to parents) are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients

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. The person taking the information from the premises accepts full responsibility for the security of the data; before sharing data, all staff members will ensure:

- That they are allowed to share it

- That adequate security is in place to protect it
- That those who will be receiving the data have been outlined in a privacy notice
- Printouts containing personal/sensitive information should be sent to the photocopier via print hold. All staff have an individual pin number to access any of their documents and immediately removed from the printer upon release/printing
- Scans are sent directly to the relevant staff member via e-mail.
- The photocopier settings ensure that no scans are stored in the memory
- Any confidential scans must be stored in the appropriate area on the office share or the member of staff's home drive.
- Confidential scans should not be saved on the staff shared area, as they cannot be password protected.
- If any confidential scans are e-mailed externally, they must be encrypted using office 365. This is done by adding the word confidential in the subject box before the subject header
- Whiteboards containing personal/sensitive information should be erased
- Any personal/sensitive/confidential documents that require shredding must be locked away securely until the documents can be destroyed
- Upon disposal personal/sensitive/confidential documents should be shredded as soon as possible by a cross cut shredding device
- The physical security of the school's buildings and storage systems, and access to them, is regularly reviewed
- If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place
- All visitors who are expected in school should be entered into the school diary. Staff should also notify the Headteacher or Deputy Headteacher and the office staff of any visitors which they are expecting. This information will be entered onto the 'weekly overview' and shared at the staff briefing meeting.
- It is very important that staff are made aware of visitors, especially when they have been invited to share the staffroom, where sensitive or confidential matters may be under discussion. Confidential information displayed on the staff noticeboard must be covered by the roller blind when visitors are expected to enter the staff room.
- All visitors should report to the office upon arrival, where they will be asked to sign in and issued with the appropriate lanyard, where necessary visitor credentials will be checked. Previous signing in information is covered with a 'discrete sheet' to ensure confidentiality. Mobile telephones will be placed in a visitor locker.
- Staff should ensure that no confidential information is on display to visitors within their working environments.
- During the school day, external doors are secured as appropriate and the office hatch is locked when not in use to prevent unauthorised access. Staff should ensure that all windows and doors are secured at the end of the school day.
- There is restricted access to the key cabinet. If staff require a key, they must be signed in and out on the key register.
- Under no circumstances are visitors allowed access to confidential personal information. Visitors to areas of the school containing sensitive information must be supervised at all times

Information Classification and Protective Marking

All Squirrel Hayes First Schools information assets will be classified into one of the three categories:

UNCLASSIFIED	OFFICIAL (PERSONAL)	OFFICIAL (SENSITIVE)
Information that is published by the school, made available to the public or that is freely available	The majority of the information that is created or processed by the school, including that related to routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media	A limited subset of the official information that could have more damaging consequences (for individuals or the school) if it were lost, stolen or published in the media, where there is a clear justifiable requirement to reinforce the "need to know"

These categories are explained in more detail below.

The classification UNCLASSIFIED

This applies only to information that rightly belongs in the public domain. This includes:

- Information that the school publishes, for example on its website
- Other information that the school makes available to its community or members of the public, even though it does not routinely publish it
- Other information the school holds that is freely available

The phrase UNCLASSIFIED should be written in capital letters when it is being used as a term to classify information. Information classified as UNCLASSIFIED must be clearly marked.

The classification OFFICIAL (PERSONAL)

All routine business operations and services should be treated as OFFICIAL (PERSONAL). The OFFICIAL (PERSONAL) classification covers information related to the following:

- The day to day business of the Trust / school, service delivery and public finances
- Safety, security and resilience
- Commercial interests, including information provided in confidence and intellectual property
- Individual people - personal information that must be protected under Data Protection legislation or other legislation (for example, health records).

The phrase OFFICIAL (PERSONAL) should be written in capital letters when it is being used as a term to classify information. Information classified as OFFICIAL (PERSONAL) must be clearly marked.

The classification OFFICIAL (SENSITIVE)

Some information which falls within the scope of the OFFICIAL classification may need a higher degree of protection than would normally be applied. This is given a stronger classification. The classification OFFICIAL (SENSITIVE) applies when:

- There could be more serious consequences (for individuals, or the school) in the event that the information is lost, stolen or published in the media

- There is a clear and justifiable requirement to restrict access solely to those who have a business need to know the information and who are within a trusted group.

The OFFICIAL (SENSITIVE) classification covers the following:

- Particularly sensitive information related to identifiable individuals, where inappropriate access could have damaging consequences (for example, information related to medical records, to investigations or to vulnerable individuals)
- Commercially sensitive information (for example, related to contracts or financial matters)
- Information that, if disclosed inappropriately, could compromise the operational effectiveness, internal stability or security of the school

The OFFICIAL (SENSITIVE) classification also applies to all information which is due to be destroyed. The phrase OFFICIAL (SENSITIVE) should be written in capital letters when it is being used as a term to classify information. Information classified as OFFICIAL (SENSITIVE) must be clearly and obviously marked.

Information combined from different sources

When information assets are gathered together from different sources, it may be the case that the individual items have different security classifications. In these cases, the overall collection of documents or files must carry the highest level of classification from the individual items. For example, if OFFICIAL (SENSITIVE) information is combined with UNCLASSIFIED information, the overall collection of information would adopt the classification OFFICIAL (SENSITIVE) and would need to be clearly marked to show that fact.

Additional guidance

Most pupil or staff personal data that is used within educational institutions will come under the OFFICIAL (PERSONAL) classification. However, some data e.g. the home address of a child at risk will be marked as OFFICIAL (SENSITIVE).

The school will ensure that all school staff, independent contractors working for it, and delivery partners, complies with restrictions applying to the access to, handling and storage of data classified as OFFICIAL or higher. When information is acquired or created, consideration must be given to how it should be classified.

All information classified as UNCLASSIFIED, OFFICIAL (PERSONAL) and OFFICIAL (SENSITIVE) must be clearly and obviously marked with its classification.

All documents (manual or digital) are to be marked with a classification will be labelled clearly within the header of the document with the wording:

"SQUIRREL HAYES FIRST SCHOOL: TITLE & DATE OF DOCUMENT" accompanied by the appropriate classification i.e.

"SQUIRREL HAYES FIRST SCHOOL: STAR Week May 2018 OFFICIAL (PERSONAL)".

Below are some examples of document control classifications for typical data processed in school.

Typical Information		Document Control
School life and events	School term times, holiday, training days, the curriculum, sports events and results, extra-curricular activities, displays of pupils work, lunchtime menus, extended services, parent consultation, homework and resources, school prospectus.	Most of this information will fall into the UNCLASSIFIED category.
Learning and Achievement	Information on how parents can support their individual child's learning, academic achievement, assessments, attainment, progress with learning, behaviour, IEPs.	Most of this information will fall into the OFFICIAL (PERSONAL) category. However, there may be learners whose personal data requires an OFFICIAL (SENSITIVE) marking, e.g. the home address of a child at risk.
Safeguarding	Information pertinent to child protection issues.	Most of this information will fall into the OFFICIAL (SENSITIVE) category, as it should only be accessed on a "need-to-know" basis.

Information must be stored securely in order to prevent unauthorised access. Stored information should be appropriately backed up to protect it against loss. Access to information classified as OFFICIAL (PERSONAL) and OFFICIAL (SENSITIVE) must be limited to those authorised to view it. Access must be granted only to those who require it in order to perform their jobs. OFFICIAL (PERSONAL) and OFFICIAL (SENSITIVE) information must always be protected against unauthorised access. This means that users must be required to supply a user name and password, or equivalent, in order to gain access to the information.

Documents must also be securely destroyed after use, e.g. shredded.

Information that is protectively marked as OFFICIAL, whether it is PERSONAL or SENSITIVE, must keep its protective marking when it is printed copied or transferred to portable media. All information protectively marked as OFFICIAL, whether it is PERSONAL or SENSITIVE, must be protected in transit and stored securely; it must not be left unattended without protection. This type of information should be printed, copied or transferred to portable media only when necessary.

Below are some examples of different uses of technology and protective marking for typical data processed in school.

Typical Information		The Technology	Notes on Protect Markings
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events.	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services.	Most of this information will fall into the UNCLASSIFIED category.
Learning and achievement	Individual pupil academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised	Typically schools will make information available by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the OFFICIAL (PERSONAL) category. There may be pupils whose personal data requires an OFFICIAL (SENSITIVE) marking. For example, the home address of a child at risk. In this case, the school may decide not to

	curriculum and educational needs.		make this pupil record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed.	Most of this information will fall into the OFFICIAL (SENSITIVE) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts i.e. about school closures would fall into the UNCLASSIFIED category.

Photographs and Videos

We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. We will always indicate our intentions for taking photographs of pupils and will obtain permission before publishing them. If we wish to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the learner. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the images or video footage and not distribute them further. Please see Squirrel Hayes First school Image and Photography Policy for more information on our use of photographs.

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

Data Retention and Disposal

Personal data will not be kept for longer than is necessary and will be disposed of securely as soon as practicable. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files.

The school may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. 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.

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

We have adopted the Information Management Toolkit for Schools created by the IRMS (Information and Records Management Society) and adhere to its principles and guidance.

Training and Awareness

All staff will receive data protection and privacy training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff

SQUIRREL HAYES FIRST SCHOOL: Data Protection Policy March 2024 (UNCLASSIFIED)

- Annual staff training
- Staff meetings / briefings
- Day to day support and guidance from the DPO, IAOs, the SLT and ICT Support.

Additional training will also be provided as part of continuing professional development, where changes to legislation, guidance or our own processes make it necessary.

Related Policies

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

- Squirrel Hayes First School Freedom of Information Policy
- Squirrel Hayes First School Information Security Policy
- Squirrel Hayes First School Technical Security Policy
- Squirrel Hayes First School Social Media Policy
- Squirrel Hayes First School Data Breach Policy
- Squirrel Hayes First School Acceptable Use Policy
- Squirrel Hayes First School Record Retention Schedule
- Squirrel Hayes First school Image and Photography Policy

Monitoring and Review

The DPO and Governing Body is responsible for monitoring and reviewing this policy. This policy will be reviewed annually or more regularly in light of any significant new developments or in response to changes in guidance.

Version No.	Date of review	Reviewer	Changes Made
01	May 2018	SE & KC	Followed LA Guidance
02	May 2019	SE	Reviewed
03	March 2020	SE	Updated form a model LA Data Protection Policy – Items added are recorded in blue
04	March 2021	SE	Reviewed
05	May 2022	EJP	Reviewed
06	May 2023	EJP	Reviewed
07	March 2024	N Rickman	Updated Legal Framework aspects Updated DPIA section
08	December 2024	N Rickman	Date Protection Officer name changed

APPENDIX A

Privacy Notice (How we use Pupil Information)

Under data protection law, 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**.

We, Squirrel Hayes First School, Springfield Road, Biddulph, Staffordshire, ST8 7DF are the 'data controller' for the purposes of data protection law.

Our Data Protection Officer is Hedda Motherwell, who can be contacted on infogov@staffordshire.gov.uk

The categories of pupil information that we collect, hold and share include, but is not restricted to:

- Personal information (such as name, unique pupil number, address, contact details, contact preferences, date of birth, identification documents)
- Characteristics (such as ethnicity, language, nationality, country of birth, free school meal eligibility and special educational needs)
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Safeguarding information
- Information relating to episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and Child Protection Plan information)
- Episodes of being looked after (such as important dates, information on placements)
- Outcomes for looked after children (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)
- Adoptions (such as dates of key court orders and decisions)
- Photographs

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

We collect and use this information

- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- To protect pupil welfare
- To administer admissions waiting lists
- To carry out research

The lawful basis on which we use this information

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

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' 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)

Where we have obtained consent to use pupils' 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 pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting pupil information

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

Storing pupil data

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. Our record retention schedule outlines how long we keep information about pupils.

A copy of our retention schedule can be found;

<http://www.squirrelhayes.staffs.sch.uk/school-policies/>

Who we share pupil information with

We routinely share pupil information with:

- Our local authority - to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- Schools that the pupil's attend after leaving us
- The Department for Education (DfE)
- The pupils family and representatives
- Our regulator - Ofsted
- Educators and examining bodies
- Suppliers and service providers - to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

Why we share pupil information

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

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

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

The National Pupil Database (NPD)

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

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

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

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

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

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

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

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

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

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

Parents and pupils' right 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.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

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.

Parents/Carers also have a legal right to access to their child's **Educational Record**. To request access please contact The School Office on 01782 973820.

You also have the right to:

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

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

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

Squirrel Hayes First School on 01782 973820 or contact the Data Protection Officer on infogov@staffordshire.gov.uk

APPENDIX B

Squirrel Hayes First School Privacy Notice (How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information
- address information
- payroll information
- emergency contact details
- performance management data
- eligibility to work in the UK documentation

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- to support continued professional development
- to safeguard and support personnel
- to aid effective communication

The lawful basis on which we process this information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- fulfil a contract we have entered into with you;
- comply with a legal obligation; and
- carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- you have given us consent to use it in a certain way;
- we need to protect your vital interests (or someone else's interests); and
- we have legitimate interests in processing the data

Where you have provided us with consent to use your data, you may withdraw this consent at any time. Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

School workforce data will not be kept for longer than is necessary and will be disposed of securely as soon as practicable.

Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Some educational records relating to former employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references.

We have adopted the Information Management Toolkit for Schools created by the IRMS (Information and Records Management Society) and adhere to its principles and guidance.

Who we share this information with

We routinely share this information with:

- our local authority
- payroll provider
- the Department for Education (DfE)
- Suppliers and service providers - to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
- Professional bodies

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

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

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

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

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

To contact the department: <https://www.gov.uk/contact-dfe>

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact **Hedda Motherwell on infogov@staffordshire.gov.uk**

You also have the right to:

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

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

Further information

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

Erica Pickford on 01782 973820 or admin@squirrelhayes.staffs.sch.uk