

# STANNINGTON INFANT SCHOOL

## General Data Protection Policy

Agreed by Governors 21.6.18

Reviewed September 2023





## Stannington Infant School Policy for General Data Protection

### Stannington Infant School Vision:

- ➊ To encourage a caring and positive attitude amongst the children towards all others and their environment.
- ➋ To provide a challenging, creative and rich curriculum which will develop curiosity, confidence and independence.
- ➌ To provide an inclusive, safe, secure, healthy and happy environment.

### Contents:

#### [Statement of intent](#)

1. [Legal framework](#)
2. [Applicable data](#)
3. [Principles](#)
4. [Accountability](#)
5. [Data protection officer \(DPO\)](#)
6. [Lawful processing](#)
7. [Consent](#)
8. [The right to be informed](#)
9. [The right of access](#)
10. [The right to rectification](#)
11. [The right to erasure](#)
12. [The right to restrict processing](#)
13. [The right to data portability](#)
14. [The right to object](#)
15. [Automated decision making and profiling](#)
16. [Privacy by design and privacy impact assessments](#)
17. [Data breaches](#)
18. [Data security](#)
19. [Publication of information](#)
20. [CCTV and photography](#)
21. [Data retention](#)
22. [DBS data](#)
23. [Policy review](#)

## Statement of intent

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

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially 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 Stannington Infant 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 UK GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Signed by:

_____	Headteacher	Date: _____
_____	Chair of governors	Date: _____

## 1. Legal framework

- 1.1. This policy has due regard to legislation, including, but not limited to the following:
  - The UK General Data Protection Regulation (UK GDPR)
  - The Freedom of Information Act 2000
  - The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
  - The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
  - The School Standards and Framework Act 1998
- 1.2. This policy will also have regard to the following guidance:
  - Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
  - Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- 1.3. This policy will be implemented in conjunction with the following other school policies:
  - [Acceptable Use policy](#)
  - [Online safety Policy](#)
  - [Freedom of Information Policy](#)

## 2. Applicable data

- 2.1. 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 UPN number. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.
- 2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

## 3. Principles

- 3.1. In accordance with the requirements outlined in the GDPR, personal data will be:
  - Processed lawfully, fairly and in a transparent manner in relation to individuals.
  - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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

#### **4. Accountability**

- 4.1. Stannington Infant School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.
- 4.2. The school will provide comprehensive, clear and transparent privacy policies.
- 4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.
- 4.4. 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 if applicable
- 4.5. The 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.
- 4.6. Data protection impact assessments will be used, where appropriate.

## 5. Data protection officer (DPO)

The DPO in conjunction with Judicum Education will:

**Data Protection Officer: Judicum Consulting Limited**

**72 Cannon Street, London, EC4N 6AE**

**Email: [dataservices@judiciumeducation.co.uk](mailto:dataservices@judiciumeducation.co.uk)**

**Lead Contact: Craig Sitwell**

5.1.

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. The DPO will have professional experience. The DPO will have knowledge of data protection law, particularly that in relation to schools.

5.3. The DPO will operate independently and will not be dismissed or penalised for performing their task.

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

## 6. Lawful processing

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

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

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

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.

- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of 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).

## **7. Consent**

- 7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- 7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- 7.3. Where consent is given, a record will be kept documenting how and when consent was given.
- 7.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- 7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- 7.6. Consent can be withdrawn by the individual at any time.
- 7.7. 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.

## **8. The right to be informed**

- 8.1. 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.
- 8.2. If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

- 8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:
- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
  - The purpose of, and the legal basis for, processing the data.
  - The legitimate interests of the controller or third party.
  - Any recipient or categories of recipients of the personal data.
  - Details of transfers to third countries and the safeguards in place.
  - The retention period of criteria used to determine the retention period.
  - The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
  - The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- 8.4. 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.
- 8.5. 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.
- 8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 8.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:
- Within one month of having obtained the data.
  - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
  - If the data are used to communicate with the individual, at the latest, when the first communication takes place.

## **9. The right of access**

- 9.1. Individuals have the right to obtain confirmation that their data is being processed.
- 9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- 9.3. The school will verify the identity of the person making the request before any information is supplied.
- 9.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- 9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.



- 9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 9.7. All fees will be based on the administrative cost of providing the information.
- 9.8. All requests will be responded to without delay and at the latest, within one month of receipt.
- 9.9. 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.
- 9.10. 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.
- 9.11. 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.

## **10. The right to rectification**

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

## **11. The right to erasure**

- 11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- 11.2. 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

- 11.3. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
- To exercise the right of freedom of expression and information
  - To comply with a legal obligation for the performance of a public interest task or exercise of official authority
  - For public health purposes in the public interest
  - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
  - The exercise or defence of legal claims
- 11.4. 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.
- 11.5. 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.
- 11.6. 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.

## **12. The right to restrict processing**

- 12.1. Individuals have the right to block or suppress the school's processing of personal data.
- 12.2. 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.
- 12.3. 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
- 12.4. 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.
- 12.5. The school will inform individuals when a restriction on processing has been lifted.

### **13. The right to data portability**

- 13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- 13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
- 13.3. 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
- 13.4. Personal data will be provided in a structured, commonly used and machine-readable form.
- 13.5. The school will provide the information free of charge.
- 13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- 13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 13.8. 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.
- 13.9. The school will respond to any requests for portability within one month.
- 13.10. 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.
- 13.11. 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.

### **14. The right to object**

- 14.1. 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.
- 14.2. 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.
- 14.3. 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.

14.4. 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.

14.5. 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.

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

## **15. Automated decision making and profiling**

15.1. 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.

15.2. 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.

15.3. 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.

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

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

## 16. Privacy by design and privacy impact assessments

- 16.1. 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.
- 16.2. 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.
- 16.3. 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.
- 16.4. 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.
- 16.5. A DPIA will be used for more than one project, where necessary.
- 16.6. 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.
- 16.7. 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
- 16.8. 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.

## 17. Data breaches

- 17.1. 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.
- 17.2. The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.
- 17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- 17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.
- 17.5. 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.

- 17.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.
- 17.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- 17.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- 17.9. 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.
- 17.10. 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
- 17.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

## **18. Data security**

- 18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, storage area with restricted access.
- 18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
- 18.3. 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.
- 18.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- 18.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- 18.6. All electronic devices are password-protected to protect the information on the device in case of theft.
- 18.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- 18.8. Where Staff and governors use their personal laptops or computers for school purposes they ensure they follow guidelines in the acceptable user policy.
- 18.9. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

- 18.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- 18.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 18.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.
- 18.13. 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.
- 18.14. Before sharing data, all staff members will ensure:
  - They are allowed to share it.
  - That adequate security is in place to protect it.
  - Who will receive the data has been outlined in a privacy notice.
- 18.15. 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.
- 18.16. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- 18.17. Stannington Infant School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- 18.18. The Headteacher is responsible for continuity and recovery measures are in place to ensure the security of protected data.

## **19. Publication of information**

- 19.1. Stannington Infant School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:
  - Policies and procedures
  - Financial information (sports funding and pupil premium report )
  - Curriculum information
- 19.2. Classes of information specified in the publication scheme are made available quickly and easily on request.
- 19.3. Stannington Infant School will not publish any personal information, including photos, on its website without the permission of the affected individual.
- 19.4. 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.

## **20. CCTV and photography**

O: Policies

- 20.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- 20.2. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
- 20.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 20.4. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- 20.5. Written permission is sought from the parent of the pupil so that the school can use images/video footage of pupils in a publication, such as the school website, social media, prospectus, or recordings of school plays.
- 20.6. Precautions, as outlined in the Photography and Videos at School Policy, are taken when publishing photographs of pupils, in print, video or on the school website.
- 20.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## **21. Data retention**

- 21.1. Data will not be kept for longer than is necessary.
- 21.2. Unrequired data will be deleted as soon as practicable.
- 21.3. 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.
- 21.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.
- 21.5. Data retention periods are identified within the asset register.

## **22. DBS data**

- 22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- 22.2. Data provided by the DBS will never be duplicated.
- 22.3. 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.

## **23. Policy review**

- 23.1. This policy is reviewed every two years by the DPO and the Governing Board.



## **Appendix 1 – Subject Access Requests**

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A data subject has the right to be informed by the School of the following: -

- (a) Confirmation that their data is being processed;
- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of the School's sources of information obtained;
- (g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
- (h) Other supplementary information.

### **How to Recognise a Subject Access Request**

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

### **How to Make a Data Subject Access Request**

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

## **What to do When You Receive a Data Subject Access Request**

All data subject access requests should be immediately directed to the headteacher who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

### **Acknowledging the Request**

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

### **Verifying the Identity of a Requester or Requesting Clarification of the Request**

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the School do not receive this information, they will be unable to comply with the request.

### **Requests Made by Third Parties or on Behalf of Children**

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;

- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

### **Fee For Responding to a SAR**

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

### **Time Period for Responding to a SAR**

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

### **School Closure Periods**

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the school is closed and there will be no one on site to comply with requests during school holiday periods. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

### **Information to be Provided in Response to a Request**

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;

- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
  - to request that the Company rectifies, erases or restricts the processing of his personal data; or
  - to object to its processing;
  - to lodge a complaint with the ICO;
  - where the personal data has not been collected from the individual, any information available regarding the source of the data;
  - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

### **How to Locate Information**

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The School should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

### **Protection of Third Parties - Exemptions to the Right of Subject Access**

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

O: Policies

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

### **Other Exemptions to the Right of Subject Access**

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

*Crime detection and prevention:* The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

*Confidential references:* The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

*Legal professional privilege:* The School do not have to disclose any personal data which is subject to legal professional privilege.

*Management forecasting:* The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

*Negotiations:* The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

### **Refusing to Respond to a Request**

The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

### **Record Keeping**

A record of all subject access requests shall be kept by the Headteacher. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

## **Appendix 2 – Subject Access Request Form**

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

### **Proof of Identity**

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

### **Section 1**

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- Birth certificate
- Driving licence
- Passport
- An official letter to my address

Personal Information

*If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*

Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

## Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- Birth certificate
- Driving licence
- Passport
- An official letter to my address

**What is your relationship to the data subject?** (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- Letter of authority
- Lasting or Enduring Power of Attorney
- Evidence of parental responsibility
- Other (give details):

## Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

--



I wish to:

- Receive the information by post\*
- Receive the information by email
- Collect the information in person
- View a copy of the information only
- Go through the information with a member of staff

\*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: [enquiries@stannington.sheffield.sch.uk](mailto:enquiries@stannington.sheffield.sch.uk)