St Nicholas' Primary School
General Data Protection Regulation (GDPR) Policy

May 2018 Review date May 2021

Contents

Statement of Intent

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

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially 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 St. Nicholas' Primary School believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. 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 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:

• Photography and Videos for use on website and newsletters

• E-safety

• Freedom of Information Policy

• Occasional public use policy e.g. local press

2. Definitions

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 IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. Sensitive personal data is referred to in the GDPR as 'special categories of personal data', including:

- Contact details
- Racial or ethnic origin
- Political opinions
- Religious beliefs, or beliefs of a similar nature
- Where a person is a member of a trade union
- Physical and mental health
- Sexual orientation
- Whether a person has committed, or is alleged to have committed, an offence
- Criminal convictions

2:3

Data subject	The person whose personal data is held or processed
Data controller	Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Headteacher. The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Data Protection Officer	See bullet point 5

3. Principles

3.1

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed with reference to OCC Retention Schedule
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998 and GDPR
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

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. St.Nicholas' Primary School will implement appropriate technical and organizational 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, which includes but is not limited to e-safety, acceptable use of IT and right of access.

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 The school will maintain its records in accordance with the accountability requirements identified by GDPR

4.5. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO will be appointed in order to:

• 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 individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

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

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

5.5. 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. The school will act as a data processor; however, this role may also be undertaken by other third parties.

6.3. 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.)

6.4. 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 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 and other government requirements such as Prevent

— Protecting the vital interests of a data subject

— The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

6.5. We hold personal information on pupils and staff where there is a substantial public interest to do so.

7. Consent

7.1. Consent will be sought prior to processing any data which cannot be done so under any other lawful basis, such as complying with a regulatory requirement.

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

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

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

7.5. 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.

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

7.7. Consent can be withdrawn by the individual at any time.

7.8. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], 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.

7.9. When gaining pupil consent, consideration will be given to the age, maturity and mental capacity of the pupil in question. Consent will only be gained from pupils where it is deemed that the pupil has a sound understanding of what they are consenting to.

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 existence of the data subject's rights, including the right to:

— Withdraw consent at any time.

— Lodge a complaint with a supervisory authority.

• The contact details of the controller (the school), and where applicable, the controller's epresentative, as well as 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.

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.

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 the third party 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

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, the third parties 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 object

12.1. 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.

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

13. Privacy by design and privacy impact assessments

13.1. 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.

13.2. 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.

13.3. 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.

13.4. 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.

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

13.6. 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

13.7. 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

13.8. 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.

14. Data breaches

14.1. 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.

14.2. 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.

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

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

14.5. 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.

14.6. 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.

14.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

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

14.9. 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.

14.10. 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

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

15. Data security

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

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

15.3. 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.

15.4. 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.

15.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

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

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

15.8. Staff and governors who use their personal laptops, mobile phones or computers for school Purpose will follow the school's agreed Code of Conduct.

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

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

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

15.12. When sending confidential information by fax or email, staff will always check that the recipient is correct before sending and when sending information out to groups of parents always use the bcc function

15.13. 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 adhering to the school's Code of Conduct. The person taking the information from the school premises accepts full responsibility for the security of the data.

15.14. 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.

15.15. 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.

15.16. 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.

15.17. St. Nicholas' School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

15.18. The school business manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data.

16. Publication of information

16.1. St. Nicholas' Primary School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

• Policies and procedures

• Minutes of meetings

• Annual reports

• Financial information

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

16.3. St. Nicholas' Primary School will not publish any personal information, including photos,

on its website without the explicit permission of the child/children's parents/carers

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

17. Photography

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

17.2. The school notifies all pupils, staff and visitors of the purpose for collecting images via notice boards, letters and email.

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

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

17.5. 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.

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

17.8 Parents/carers are asked not to put pictures or videos of other people's children or their own children where other children are in the frame on social media without the express permission of the other child/children's parents.

18. Data retention

18.1. Data will not be kept for longer than is necessary.

18.2. Unrequired data will be deleted as soon as practicable.

18.3. 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.

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

19. DBS data

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

19.2. Data provided by the DBS will never be duplicated.

19.3. 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.

20. Policy review

20.1. This policy is reviewed every two years by the SBM and the headteacher.

The next scheduled review date for this policy is May 2021.