St. Nicholas C of E Primary School

Data Protection Policy

Our Vision Statement

"To maximise the learning potential of every pupil within the love of God."

Date reviewed:	June 2021
Reviewed by:	R. Younger
Approved by Headteacher:	June 2021
Date of next review:	Summer 2022

Contents

1. Introduction

1.1 St Nicholas C of E Primary School collects and uses personal data about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use personal data to ensure that the school complies with its statutory obligations.

1.2 Schools have a duty to be registered as data controllers with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website www.ico.org.uk
The school's business manager acts as the representative of the data controller on a day-to-day basis.

1.3 Schools also have a duty to issue a privacy notice to all pupils/parents, to members of the school workforce (including governors) and to volunteers for whom they hold personal data; this summarises the personal data that is held, why it is held and the other parties to whom it may be passed on.

2. Purpose

2.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and other related legislation. It will apply to all personal data regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

2.2 All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3. What is Personal Data?

3.1 Personal data is defined as "Any information relating to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person."

3.2 Special category personal data includes information about a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation. Special category personal data is personal data which the UK GDPR says is more sensitive and so needs more protection.

4. Data Protection Principles

4.1 The UK GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) 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;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and
f) 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.

4.2 The school is committed to maintaining the above principles at all times. Therefore the school will:

- regularly check the quality and the accuracy of the personal data it holds;
- ensure that information is not retained for longer than is necessary and according to the school's retention schedule;
- ensure that when obsolete data is destroyed that it is done so appropriately and securely;
- ensure that clear and robust safeguards are in place to protect personal data from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- share personal data with others only when it is legally appropriate to do so;
- set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests;
- ensure our staff are aware of and understand our policies and procedures;
- implement measures that meet the principles of data protection by design and default, such as:
  - data minimisation
  - pseudonymisation
  - transparency
  - continuously creating and improving security features;
- provide comprehensive, clear and transparent privacy notices;
- use data protection impact assessments where appropriate;
- maintain records of activities relating to higher risk processing, such as those which:
  - 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.

4.3 Internal records of processing will include the following:

- description of the categories of individuals and personal data;
- purpose(s) of the processing;
- lawful basis for processing;
- description of technical and organisational security measures;
- details of transfers ~~outside the EU,~~ to third countries or international organisations.

5. Data Security

5.1 Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access, and will not be left unattended or in clear view anywhere with general access.

5.2 Digital data is coded, encrypted or password-protected. Network drives are regularly backed up both on-site and off-site. Access to data stored in the cloud requires 2 factor authentication. The school has a Firewall in place which includes anti-virus, anti-spam, anti-malware, content and URL filtering. The use of memory sticks has been disabled on school devices. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

5.3 All necessary staff are provided with their own secure login and password to enable access to the school network; different levels of access are enabled for different staff, according to what information they have a right to view and/or edit. Passwords must be changed at least every 13 weeks or accounts will be automatically locked.

5.4 Where possible, staff and governors will not use their personal devices for school purposes. If personal devices are used, staff and governors must ensure that they do not download any school-owned data to the device. If staff and governors wish to access their school email account on their smartphone, this must only be done via the Outlook app and fingerprint authentication / face ID must be enabled within the app.

5.5 Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient. Circular emails to parents are sent blind carbon copy (bcc) so that email addresses are not disclosed to other recipients. When sending emails, staff must always check that the recipient is correct before sending.

5.6 Before sharing personal data, all staff members must ensure that:

- They are allowed to share it;
- They have verified the identity of the person / organisation they are sharing the data with;
- Adequate security is in place to protect it.

5.7 When disposing of personal data, paper documents will be shredded. When digital storage devices are no longer required the school arranges for collection by a WEEE compliant computer recycling and disposal company. If devices are reusable, data wiping, stripping and shredding takes place to ensure all data is removed before refurbishing for circulation. Devices that are not reusable have all data destroyed by destroying the hard drives.

5.8 Details of how the school deals with breaches of personal data are in the school's Data Breach Policy & Procedure.

5.9 The school takes its duties under UK data protection laws seriously and any unauthorised processing of personal data by staff may result in disciplinary action.

6. Data Protection Officer

6.1 Under the definition provided in Section 7 of the DPA, St Nicholas C of E Primary School is a public authority and is therefore required to appoint a Data Protection Officer (DPO). The contact details for our DPO are contained in all our privacy notices.

7. Subject Access Requests

7.1 Individuals (data subjects), including children, have the right to obtain confirmation that their data is being processed by the school and the right to submit a subject access request to gain access to their personal data.

7.2 There is no prescribed format for subject access requests. Where a subject access request has been made electronically, the information will be provided in a commonly used electronic format, unless otherwise specified by the data subject.

7.3 Where deemed necessary, the school will seek to verify the identity of the requester before the disclosure of any information, including checks regarding proof of relationship to the child where relevant.

7.4 Requests for information by an adult about a pupil will only be considered if the adult making the request has parental responsibility for that child. Subject access requests made by adults on behalf of a child for whom they have parental responsibility will be considered on a case by case basis, according to the ICO's current guidance.

7.5 In the event that a large quantity of information is being processed about an individual, the school will ask the requester to specify the information that the request is in relation to.

7.6 A copy of the information will be supplied to the requester free of charge; however, the school may impose a reasonable fee to comply with requests for further copies of the same information.

7.7 Where a request is manifestly unfounded, excessive or repetitive, the school holds the right to either request a reasonable fee to deal with the request or to refuse to deal with the request.
In the event that the school decides to charge a fee, the requester will be informed of this decision promptly and the request will not be dealt with until the fee has been received.
In the event that the school decides to refuse to deal with the request, the requester will be informed of this decision and the reasoning behind it, as well as their right to complain to a supervisory authority or to a judicial remedy, within one month of the refusal.

7.8 All fees will be based on the administrative cost of providing the information.

7.9 There are certain types of information, that the school may hold, which are exempt from the DPA and which, therefore, the school does not have to grant subject access to. More information about this is available from the ICO.

8. Parent's Right of Access to their Child's Educational Record

8.1 The Education (Pupil Information) (England) Regulations 2005 give a parent their own independent right to a copy of their child's educational record.

8.2 The Regulations provide a legal definition of an 'educational record'. The definition is wide and includes, regardless of its form, any information about current and past pupils that is processed by or for the school's governing body or any teacher at the school.

8.3 A response will be given to such a request from a parent within 15 school days, as per the Regulations.

8.4 There are certain types of information, that the school may hold, which are exempt from disclosure under these Regulations. More details can be found at http://www.legislation.gov.uk/uksi/2005/1437/contents

9. Safeguarding

9.1 St Nicholas C of E Primary School understands that UK data protection legislation does not prevent or limit the sharing of information for the purposes of keeping children safe.

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

- Whether data was shared;
- What data was shared;
- With whom data was shared;
- For what reason data was shared;

- Where a decision has been made not to seek consent from the data subject or their parent;
- The reason that consent has not been sought, where appropriate.

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

10. CCTV

10.1 The school has a number of Closed Circuit Television (CCTV) cameras on site, and a recording system connected to these cameras.

10.2 We use the CCTV system to monitor and collect visual images for security and the prevention of crime. We also use the CCTV system for the purpose of maintaining good order in the school.

10.3 The recording system is held securely in a locked room, and access to view live footage and recordings is password protected. Only authorised persons have this password.

10.4 Viewing of live footage and recordings only takes place in restricted areas, where only authorised persons can view the images.

10.5 In certain circumstances, it may be necessary for the school to share information from the CCTV system with the police or another law enforcement agency.

10.6 Individuals whose information is recorded on the school's CCTV system have a right to be provided with that information or, if they consent to it, view that information. See Section 6 of this policy.

11. Protection of Biometric Information of Children

11.1 The UK GDPR defines biometric data in Article 4(14):

> "'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

The term 'dactyloscopic data' means fingerprint data.

11.2 The processing of children's biometric information in schools is subject to the provisions of the Protection of Freedoms Act 2012, as well as the DPA.

11.3 St Nicholas C of E Primary School does not process any biometric information of children.

12. Complaints

12.1 Complaints relating to this policy will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the ICO (the statutory regulator) www.ico.org.uk or telephone 0303 123 1113.