Nutley Church of England Primary School

Data Protection and Information Security Policy

This policy was endorsed by the **Board of Governors** at the meeting on 19th July 2021

Head Teacher signed: 

Chair of Governors signed: 

This policy will be reviewed annually and revised where necessary- Date: July 2022

1. Introduction

Nutley CE School collects and uses personal information about staff, governors, volunteers, pupils and parents. This information is collected so that the school can provide education in a secure environment. Schools have a legal requirement to gather process and share information to enable the school to meet its statutory obligations.

The purpose of this Policy is to ensure the school (Governors, Senior Leaders and Staff) has identified how it will collect, secure, process, share and erase data in accordance with the requirements of the General Data Protection Regulation.

This policy relates primarily to the personal data of individuals that would enable them to be identified directly or indirectly by an identifier such as name, ID number, unique pupil number, address), or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Sensitive Personal data (Special Category Data) requires extra protection and includes any information that may identify any of the following information about the individual:

- racial or ethnic origin
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation
- genetic/biometric identifier

2. The Regulator

The Information Commissioner's Office is responsible for:

- overseeing compliance with Data Protection legislation
- supporting organisations to become compliant
- enforcing the legal processing of data
- investigating complaints where organisations are not compliant

Schools must register with the ICO and maintain a current record of the information it is processing, the legal basis for processing the information and who it is being shared with.

3. Compliance with the Principles of GDPR

The school will ensure all information collected, processed, shared and stored complies with the principles of GDPR. This means Personal Identifiable Information will be:

- processed lawfully, fairly and in a transparent manner
- collected and used only for the legitimate purpose it was collected
- only collected if required for the legitimate purpose
- accurate and where required, rectified without delay

- kept only as long as it is required in accordance with the school's retention schedule
- appropriately secured against unauthorised or unlawful processing, accidental loss, destruction or damage
- processed in accordance with the rights of data subjects
- processed in the European Economic Area unless additional protection has been put in place

4. The school's commitment to the principles of GDPR

The school is committed to maintaining the GDPR principles at all times and will:

- Inform individuals why their information is being collected
- Inform individuals when their information is shared, why it is being shared and with whom
- Check the quality and the accuracy of the information it holds
- Only retain information for as long as it is required
- Erase data securely when no longer required
- Ensure safeguards are in place to protect personal information from loss, theft and unauthorised disclosure
- Only share information when it is legally appropriate to do so
- Enable access to individual records through its Subject Access Request process
- Ensure all staff understand the school's policies and procedures

5. Responsibilities

All employees, Governors and any other individual handling personal information on behalf of the school have a responsibility to ensure that they comply with Data Protection legislation and the school's policies.

The school ensures that all staff who are involved in processing personal data undertake training as part of their Induction and the school provides mandatory data protection training as part of its Safeguarding responsibilities.

6. The legal basis

The school will comply with all relevant UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Legislation (Data Protection Act 1998, GDPR, Data Protection Act 2018)
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Act 1974
- Privacy and Electronic Communications (EC Directive) Regulations 2003

7. Keeping Data Safe

Before introducing a new policy, procedure, system or database involving personal data the school will complete a Data Protection Impact Assessment (DPIA). The DPIA will identify any potential risks of harm to individuals through the misuse of their personal information, allowing these risks to be reduced. A DPIA will be conducted in all cases where processing is likely to result in a high risk to individuals.

8. Provision of Individual Rights of the data subject

8.1. Right to be Informed

The school's Privacy Notices explain what information is being processed, the legal basis for processing, the purpose of processing, who the information is shared with and the schedule detailing how long the information is held. The Privacy Notice for Parents and Pupils is available on the school's website.

8.2. Right of Access

Individuals have the right to request access to information relating to them. This right is called a Subject Access Request. An individual can request information by submitting a request in writing to the school.

Parents may make requests on behalf of their children but if the child is 13 years or older, the child must also provide written consent for the parent to make the application on their behalf.

An application on behalf of anyone lacking mental capacity who would otherwise have the right to request access to their records may be made where a nominated person making the application can provide a Lasting Power of Attorney or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

Only information relating to the individual will be disclosed as part of a subject access request.

Any information that may prejudice the prevention and detection of crime may be exempted from disclosure. There are also a number of other exemptions which may be applied and these will be explained on an individual basis.

An individual can make a Subject Access Request by completing the form on the school website.

Requests will be processed within 1 month of receipt

Where a request may be considered complex the applicant will be notified of this within the initial 1-month period and a response will be provided within a further 2 months. A complex case may be as follows:

- retrieval and appraisal of information from multiple sources
- retrieval of large volumes of information for one data subject

- which are difficult to separate from information relating to other data subjects
- it is one in a series of requests from the same individual
- it involves the release of third party data for which consent has been
- refused or cannot be obtained Right to object

8.3. Right to object

Data subjects have the right to object to their information being processed if they do not believe there is a legitimate legal basis for processing or their data is being shared without a legitimate purpose.

8.4. Right to rectification

Individuals have the right to have any personal data rectified if it is incorrect. This includes the need to ensure that the data held is complete.

8.5. Right to restriction

Individuals have the right to request the temporary restriction of the processing and access to their data. This might apply when:

- the accuracy of data is being established,
- confirming the validity of an objection to the school processing the data.
- data has been processed unlawfully but the data subject does not want us it erased.
- it is no longer required by the school but the individual has requested the information be retained in connection with a legal claim.

The right to restrict data does not apply if the school requires the information in connection with a legal claim of there is a legal basis for continuing to process the data.

8.6. Right of erasure

Where there is no justification for the continued use of an individual's data, they may ask for it to be erased. Data may be erased when:

- It is no longer required for the purpose for which it was collected
- Consent for the original processing has been withdrawn, including parental consent given on behalf of a child, who no longer wishes the data to be held
- It has been processed without a legitimate legal basis
- There is a legal requirement to erase the data

The school will decline a request for erasure when:

- A legitimate legal basis exists for processing the data
- The information is required for public health reasons
- The data is required for historic, statistical or archiving activities
- The data is required in connection with a legal claim

8.7. Right to portability

Where data is held electronically, forms part of a contract and consent for processing has been given by the individual – individuals can ask for their data to be transferred electronically to another organisation.

8.8. Automated Processing

The school does not use IT systems to make automatic decisions based on personal data.

9. Data Protection Breach

The school will take all preventable steps to hold and process individual data securely. In the unlikely event of a breach, the school has a data breach management process which all staff are aware of and have received appropriate training so they can recognise and react appropriately to a data breach. All breaches of Data Protection legislation will be reported to the school's Data Protection Officer who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary.

10. Information security

Information that is confidential but doesn't relate to an individual or individuals includes the following:

- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Any information which, if released, could cause problems or damage to individuals, the public, the school or another organisation. This could be personal, financial, reputation or legal damage.

The school's Information Security Policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

It applies to all employees, Governors, volunteers and staff of service delivery partners who handle information for which the school is responsible. It forms the basis of contractual responsibilities in contracts with Data Processors where reference is made to the school's Data Protection and Information Security Policy.

The school will maintain the confidentiality, integrity and security of all data ensuring it is gathered, secured, stored, shared and erased in accordance with the data protection regulation. The school will review its data protection policies as part of its governance process. It will also check the effective implementation of these policies through the regular Governor led Safeguarding Audits.

Information systems will be checked regularly for technical compliance with relevant security implementation standards.

Operational systems are subjected to technical examination to ensure that hardware and software controls have been correctly implemented.

Please see Appendix 1.

11. Management of Information

The School will manage information in accordance with the principles and procedures within this policy and other relevant policies and standards. The following principles apply to how we handle information in the school:

- All identifiable personal information is treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.
- Procedures will be maintained to ensure compliance with Data Protection legislation, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information is recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

12. School records

We will create and maintain adequate pupil, staff and other records to meet the school's business needs and to account fully and transparently for all actions and decisions. Such records can be used to provide credible and authoritative evidence where required; protect legal and other rights of the school, its staff and those who have dealings with the school; facilitate audit; and fulfil the school's legal and statutory obligations.

Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner, in line with the school's Records Management and Electronic Records Management policies.

13. Protection of Biometric information for children

The DfE provide guidance on the Protection of biometric information of children in schools and colleges under Protection of Freedoms Act 2012 and Data Protection Act 2018

The written consent of at least one parent must be obtained before the biometric data is taken from the child and used. This applies to all pupils in schools and colleges under the age of 18.

In no circumstances can a child's biometric data be processed without written consent. The school will not process the biometric data of a pupil (under 18 years of age) where:

a) the child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

b) no parent has consented in writing to the processing; or

c) a parent has objected in writing to such processing, even if another parent has given written consent.

The school will where possible provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system.

The latest guidance published by the DfE for the implementation of this aspect of policy is available via the following link:

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

14. Contacts

The Data Protection Officer for the school is:

Roger Simmons – GDPR Practitioner and DPO
07704-838512
rsimmonsltd@gmail.com

Office of the Information Commissioner
The Information Commissioners, Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF
website: www.ico.gov.uk

Appendix A

Data Protection & Information Security Policy.

Annex A - Standards for handling confidential information

Standards for handling confidential information

The following standards are set out for all members, employees and service delivery partners as the minimum standards for handling sensitive and

confidential information. Failure to adhere to these standards may result in disciplinary or other appropriate action.

A.1 Creation/acquisition

When information is acquired and records created there are some simple principles we will follow:

We will ensure that it is:

• accurate (factual or qualified expert opinion)
• up to date (changes updated as soon as possible)
• consistent (the same information across different datasets)
• relevant (only as much and for as long as needed for the intended purpose)

When acquiring and handling personal information we will comply with the processes and standards set out under Data Protection legislation.

A.2 Maintenance and use

Information and records will be maintained to ensure that they are accurate, up to date and consistent. When using confidential information there are some ground rules we will follow to maintain confidentiality and integrity:

• we will never leave the information where others could see it e.g. on a desk, computer screen or left on a fax or printer
• we do not discuss the information where others not authorised may overhear
• we only use the information for the purpose for which it was collected
• changes will be recorded as soon as possible after the change occurs
• we will always store information securely, following filing procedures in structured file systems
• we will always put the information/records back as soon as they have been finished with
• we do not produce copies unless they are needed and always update the master record, securely destroying copies as soon as they are no longer needed
• we will review the information regularly to ensure it is accurate and up-to-date
• if information and records are taken from a secure location the risk of loss increases and we will follow the standards set out in the Data in Transit policy

A.3 Disclosure

Prior to disclosure of personal or commercially confidential information we will be satisfied that at least one of the following applies:

• for personal data, requirements of Data Protection legislation are

satisfied (see Data Protection – Guidance for Employees)
• disclosure is permitted under an exemption set out in Data Protection legislation; (e.g. the prevention or detection of crime, the capture or prosecution of offenders, and the assessment or collection of tax or duty)
• disclosure is in the public interest, (e.g. for safeguarding national security or for preventing harm to children or adults)
We will never disclose confidential information to anyone who does not have a right to see it.
If we are unsure we will not disclose the information. We will seek advice from a manager, departmental Information Governance or Information Security lead or Data Protection Officer.

A.4 Storage

All confidential information must be stored securely and access allowed only to those who need it for legitimate purposes.
Secure storage can be secure buildings with access controls to the building, specific floors and individual offices. The controls can be swipe cards, keypads, key locks etc. Appropriate measures must be used depending on the sensitivity of the information and who should have access to it.
Similarly access to electronic information must be controlled by the use of passwords and assigned permissions within the systems that hold the information.
To ensure appropriate access under these controls we MUST NOT let others use our access whether it is a swipe card, key, login or system password or other access control.

A.5 Disposal

When disposing of any sensitive and confidential information we will comply with the Council's Retention and Disposal Schedules for the specific information and records being disposed.
When disposing of confidential information we will always use secure methods such as cross-cut shredding or pulping or the confidential waste bins where available and keep the waste in a secure place until it can be collected for secure disposal. We will NEVER put sensitive and confidential waste in normal waste bins.