THE FEDERATION OF NETTLESTONE AND NEWCHURCH PRIMARY SCHOOLS

# DATA PROTECTION POLICY

Revision: 8~~7~~

Date Agreed: April 2026~~May 2025~~ Review Date: April 2027~~6~~

Co-Chair of Board of Governors

Executive Headteacher

All the Governors and staff of The Federation of Nettlestone & Newchurch Primary Schools are committed to sharing a common objective to help keep the children and staff of the school community safe. We ensure that consistent effective safeguarding procedures are in place to support families, children, and staff of the school.

## Table of Contents

Table of Contents 2
Document Control 3
Introduction 3
Legislation and Guidance 3
Definitions 4
Term 4
Definition 4
The Data Controller 4
Data Protection Officer 5
Data Protection Principles 5
Roles and Responsibilities 5
General Staff Guidelines 6
Consent 6
Data Storage 7
Data Use 7
Data Accuracy 8
User Rights 8
Subject Access Requests 9
Parents Requesting Information about Children 9
Accessing Personal Information on Someone Else's Behalf 9
Disclosing Data for Other Reasons 9
Providing Information 10
Monitoring Arrangements 10
Links with Other Policies 10
Appendix A – Privacy Notice for Pupils 11
Appendix B – Privacy Notice for Staff 13

## Document Control

| Policy Owner: RP | | | | |
|---|---|---|---|---|
| Revision | Date Issued | Prepared By | Approved | Comments |
| 1 | Jan 2018 | DR | FGB | Formulation of policy in line with model policy from ICO. |
| 2 | Mar 2018 | KJH/HB/RP | | Adaptations in light of Data Officer monitoring and changes required for the introduction of the General Data Protection Regulation 2018 (applicable from 25/05/18). Policy updated in line with IOW Council SLA for Data Protection & Data Processing. |
| 3 | July 2019 | KJH/RP | | Minor amendments. |
| 4 | July 2020 | RP | | Minor amendments including removal of hyperlinks. |
| 5 | Mar 2023 | RS | PC | Amendments made following recommendation from DPO. |
| 6 | Jun 2023 | | PC | Change of personnel in SBM role. |
| 7 | May 2025 | MJ | PC | Periodic review. No changes needed. |
| 8 | May 2026 | MJ | PC | Periodic review. No changes needed. |

## Introduction

1. Our Federation aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the *Data Protection Act 2018* and the *General Data Protection Regulation (GDPR) 2018.*
2. This policy applies to all data regardless of whether it is in paper or electronic format.
3. This policy is designed to ensure that the Federation:
   - Complies with data protection law and follows good practice.
   - Protects the rights of staff, pupils and partners.
   - Is open, honest and transparent about how it retains and processes the data of each individual.
   - Protects itself from the risk of a data breach.

## Legislation and Guidance

4. This policy meets the requirements of the *Data Protection Act 2018* and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department of Education. It also considers the provisions of the *General Data Protection Regulations*, *2018*.
5. In addition, this policy complies with *Regulation 5* of the *Education (Pupil Information)(England) Regulations 2005*, which gives parents the right of access to their child's educational record.

6. These rules apply regardless of whether data is stored electronically, on paper or any other materials.

7. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

## Definitions

| Term | Definition |
|---|---|
| Personal Data | Data from which a person can be identified including data that when combined with other readily available information leads to a person being identified. (As set out in Article 4(1) of the GDPR.) |
| Sensitive Personal Data | Data such as:<br>• Contact details.<br>• Racial or ethnic origin.<br>• Political opinions.<br>• Religious beliefs, or beliefs of a similar nature.<br>• Where a person is a member of a Trade Union.<br>• Physical and mental health.<br>• Sexual orientation.<br>• Whether a person has committed, or is alleged to have committed, an offence.<br>• Criminal convictions. |
| Processing | Obtaining, recording or holding data. (As set out in Article 4(2) of the GDPR). |
| Data Subject | The person whose personal data is held or processed. |
| Data Controller | A person or organisation that determines the purposes for which, and the manner in which, personal data is processed. (As set out in Article 4(7) of the GDPR). |
| Data Processor | A person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller. (As set out in Article 4(8) of the GDPR). |
| Data Protection Officer | A person who will assist to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. (As set out in Article 37-39 & 83 of the GDPR). |

## The Data Controller

8. The Federation of Nettlestone and Newchurch Primary Schools processes personal information relating to pupils, staff and visitors and therefore is a Data Controller.

9. It is the responsibility of the Data Controller to 'implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that processing is performed in accordance with the regulation.'

10. Each school is registered as a Data Controller with the Information Commissioner's Office (ICO) and renews this registration annually.

## Data Protection Officer (DPO)

11. The DPO is the Assistant Director of Corporate Services at the Isle of Wight Council and can be contacted by emailing dpo@IOW.gov.uk.

12. The DPO must 'have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.'

## Data Protection Principles

13. The *Data Protection Act 2018* is based on the following data protection principles, or rules, for good data handling:

- 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.
- Personal data shall be processed in accordance with the rights of data subjects under the *Data Protection Act 2018*.
- 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 of 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.

## Roles and Responsibilities

14. Everyone who works with the Federation has some responsibility for ensuring data is collected, stored and handled appropriately.

15. Everyone that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

16. The Governing Body is ultimately responsible for ensuring the Federation meets its legal obligations.

17. The Executive Headteacher working alongside the nominated Data Officer (Hannah Berners) is responsible for:

- Keeping the Governing Body and staff updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies in line with an agreed schedule.
- Arranging Data Protection training and advice for all covered by this policy if required and requested.
- Managing data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that the Federation holds about them (Subject Access Requests).

- Checking and approving contracts or agreements with third parties that may handle the Federation's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet the acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services that the Federation is considering using to store or process data. For instance, cloud-based computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets in line with Local Authority (LA) legal guidance.
- Notify, where feasible within 72 hours, the ICO of any 'high risk' data breach. A reasoned justification must be provided if this timeframe is not met. The Data Controller must also notify the affected Data Subjects without undue delay.

## General Staff Guidelines

18. The following guidelines should be followed by all staff within the Federation:

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- The Federation will provide training for all employees to help them understand their responsibilities when handling data when required or requested.
- Employees should keep all data secure by taking sensible precautions and following the guidelines illustrated in the policy.
- In particular strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people either within the Federation or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required it should be deleted and disposed of in line with our record management guidance.
- Employees should request help from their line manager or the Data Protection Controller or Officer if they are unsure about any aspect of data protection.
- Data Processors will have direct legal obligations and responsibilities which means that Processors can be held liable for data breaches.
- When no longer needed, inaccurate or out of date data will be disposed of securely as per our records management policy.

## Consent

19. Some processing of personal data relies upon consent. Where this is the case a data subject's consent to the processing of their personal data must be freely given, specific, informed and unambiguous.

20. Parental consent is required for the processing of personal data of children under the age of 16. Parental consent is not required in the context of preventative or counselling services offered directly to a child, including where they may be at risk of harm (e.g., to police or children's services).

21. Consent should be explained in simple terms. Silence or inactivity does not constitute consent. Clear and affirmative consent to the processing of private data must be provided.

22. Consent must be explicit for sensitive data. The Data Controller is required to demonstrate that consent was given. Existing consents still work provided they meet the conditions of the new regulations.

23. Parents have the right to withdraw consent to the collection, processing and transfer of personal information for a specific purpose. They have the right to withdraw at any time. Upon written notification of the withdrawal the Federation will no longer process information for that individual for the purposes that were originally agreed to unless there is another legitimate basis for doing so in law.

## Data Storage

24. These rules describe how and where data should be safely stored. Questions about storing data can be directed to Wight Support or the Data Controller.

25. When data is stored on paper it should be kept in a secure place where unauthorised people can not see it.

26. These guidelines also apply to data that is usually stored electronically but may have been printed out for some reason:

- When not required the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between employees. They should be ideally eight characters long and contain letters and numbers.
- If data is stored on removable media (e.g., CD, DVD, USB stick) these should be kept locked away securely when not being used and encrypted with appropriate software.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.
- A risk-based approach must be adopted before undertaking higher risk data processing activities. Data Controllers are required to conduct Privacy Impact Assessments where privacy breach risks are high to analyse and minimise the risks to their Data Subjects.

## Data Use

27. Personal data is of no value to the Federation unless the staff can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular it should never be sent by email as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. Wight Support can explain how to send data to authorised external contacts e.g., by password protection.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers and always access and update the central copy of any data.

## Data Accuracy

28. The law requires the Federation to take reasonable steps to ensure data is kept accurate and up to date.

29. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

30. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

31. Staff should take every opportunity to ensure data is updated. For instance, by confirming a parent's details when they call.

32. The Federation will make it easy for data subjects to update the information that each school holds about them.

33. Data should be updated as inaccuracies are discovered. For instance, if a governor can no longer be reached on their stored telephone number it should be removed from the database.

34. The amount of personally identifiable information shared should be reduced to a minimum and ensure that it is not stored for any longer than is necessary. Data privacy encompasses other factors that could be used to identify an individual such as their genetic, mental, economic, cultural or social identity.

## User Rights

35. Data Controllers must inform and remind users of their rights as well as documenting the fact that they have reminded them of their rights. By law each user has the right to:

    - Request access to their personal information (commonly known as a Subject Access Request). This enables the user to receive a copy of the personal information that is held about them within the Federation to check that staff are lawfully processing it.
    - Request correction of their personal information. This enables the user to have any complete or incomplete or inaccurate information held by the Federation corrected.
    - Request erasure of their personal information. This enables the user to ask the Federation to delete or remove personal information where there is no good reason to continue to process it.
    - Object to processing of their personal information where the Federation is relying on a legitimate interest (or those of a third party) and there is something about the user's particular situation which makes them want to object to processing on this ground.
    - Request the restriction of processing of their personal information. This enables the user to ask the Federation to suspend the processing of personal information about them for example, should the user want the Federation to establish its accuracy or the reason for processing it.
    - Request the transfer of your information to another party.

36. Where consent for data processing is relied upon users should not have to opt out of their data being used, they must opt in our systems.

37. Data portability allows a user to request a copy of their personal data in a format usable by them and electronically transmissible to another processing system.

38. Should a user wish to review, verify, correct or request erasure of their personal information, object to processing of their personal data or request that the Federation transfer a copy of their personal information to another party a request in writing should be made to the Executive Headteacher.

39. Users will not usually have to pay a fee to access their personal information (Subject Access Request). The Data Controller will aim to provide the relevant data within a calendar month for any data subject requests. Any Education Regulations requests will be responded to within 15 school days.

## Subject Access Requests

40. Individuals should include the following information when making Subject Access Requests:

- Full name, address, contact telephone number and email address.
- Any information used by the Federation to identify or distinguish the individual from others of the same name (i.e., account numbers, unique ID's etc.)
- Details of the specific information required and any relevant dates.

41. The Data Controller will always verify the identity of anyone making a Subject Access Request.

42. The Federation will provide the information requested in writing where possible, unless it takes 'disproportionate effort' or if the individual agrees to some other form such as seeing it on screen.

43. The Federation will provide any personal information that is held about an individual following the principles of the ICO Subject Access Code of Practice.

## Parents Requesting Information about Children

44. Information about children may be released to a person with parental responsibility. However, the best interests of the child will always be considered.

45. Even if a child is very young data about them is still their personal data and does not belong to anyone else. It is the child who has a right of access to information held about them.

46. Before responding to a request for information held about a child the Federation will consider whether the child is mature enough to understand their rights. If the Federation is confident that the child can understand their rights then it will respond to the child rather than the parent. What matters is that 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.

## Accessing Personal Information on Someone Else's Behalf

47. The Data Protection Act allows a request to be made on someone else's behalf. This is often necessary for a solicitor acting on behalf of a client or it could be that an individual would like someone to act for them.

48. In these cases, the Federation will need to satisfy itself that the third party making the request has the individual's permission to act on their behalf. It is the third party's responsibility to provide this evidence which could be written authority to make the request or a power of attorney.

49. If a person does not have the mental capacity to manage their own affairs and the third party is their attorney, they will have the right to access information about the person they are representing to help them carry out the role. The same applies to a person appointed to make decisions about such matters.

- In England and Wales – by the Court of Protection.
- In Scotland – by the Sheriff Court.
- In Northern Ireland – by the High Court (Office of Care and Protection).

## Disclosing Data for Other Reasons

50. In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the Data Subject. Under these circumstances the Federation will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the LA and from the Federation's legal advisers where necessary.

## Providing Information

51. The Federation aims to ensure that individuals are aware that their data is being processed and that they understand how the data is being used and how to exercise their rights.

52. To these ends the Federation has a Privacy Statement, setting out how data relating to individuals is used by the Federation (See Appendix A). This will be issued to parents upon pupil admission to school and annually thereafter. A similar Privacy Statement will be issued to staff upon appointment to the Federation and reviewed as part of the September induction process each year (see Appendix B).

## Monitoring Arrangements

53. The Governing Body is responsible for monitoring and reviewing this policy.

54. The Executive Headteacher and Data Officer will check that the school complies with this policy by, among other things, reviewing schools records annually.

55. This document will be reviewed annually. At every review the policy will be shared with the Governing Body.

## Links with Other Policies

56. This Data Protection Policy and Privacy Notice is linked to the following:

- Freedom of Information Publication Scheme
- Record Management Policy.
- Safeguarding Policy.
- Child Protection Policy.
- Safe Recruitment Policy.

# Appendix A – Privacy Notice for Pupils

THE FEDERATION OF NETTLESTONE AND NEWCHURCH PRIMARY SCHOOLS

## PRIVACY NOTICE FOR PUPILS

### How We Use Pupil Information

This school is a member of the Federation of Nettlestone & Newchurch Primary Schools and is registered as a Data Controller with the Information Commissioner's Office (Registration Number: A8274268 (Nettlestone) and Z9897909 (Newchurch) for the purposes of the Data Protection Act 1998 and General Data Protection Regulations 2018.

We collect information from you about your child(ren) and may receive information about them from their previous school/academy/setting, the Local Authority, other Local Authorities and/or the Department of Education (DfE). We also share it with these agencies to comply with our statutory duties.

We hold this personal data and use/share it to:

- Support your child(ren)'s teaching and learning.
- Monitor and report on their progress.
- Contribute to improving your child(ren)'s health and reducing inequalities.
- Provide appropriate pastoral care.
- Statistical forecasting and planning.
- Assess how well the school/ Federation is doing.

This information includes contact details, assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, nationality, any special educational needs and relevant medical information.

**We will not give information about your child(ren) to anyone outside the Federation without your consent unless the law allows us to i.e., in the case of safeguarding.**

We have local arrangements in place where the Federation exchanges information with outside agencies which may include but are not exclusively restricted to medical professionals, extended school and pre-school providers, Early Years team, Early Help/MASH Team, Educational psychologists, speech therapists and Children's Services.
If you want to see a copy of the information about your child(ren) that we hold and/or share, please contact the school office. Child protection information will not be released unless cleared by Children's Services and/or Isle of Wight County Council Legal Department to do so.

We follow the Data Protection Policy of the Federation of Nettlestone and Newchurch Primary School. A copy of this policy is available from the Executive Headteacher, Miss Kirsty Howarth or on the school's website: www.nettlestoneprimaryschool.co.uk or www.newchurchprimaryschool.co.uk

We are required by law to pass some information about your child(ren) to the Department for Education (DfE). This information will, in turn, then be made available for use by the Local Authority. The DfE may also share pupil level personal data that we supply to them with third parties. This will only take place where the law allows it to do so and it follows the Data

Privacy Notice - Pupils

THE FEDERATION OF NETTLESTONE AND NEWCHURCH PRIMARY SCHOOLS

Protection Act 1998 and General Data Protection Regulations 2018. Decisions on whether the DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: **https://www.gov.uk/guidance /national-pupil-database-apply-for-a-data-extract**

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government /publications/national-pupil-database-requests-received.

If you require more information about how the Local Authority (LA), or DfE collect, store and use your information, then please go to the following websites: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

Privacy Notice - Pupils

## Appendix B – Privacy Notice for Staff

THE FEDERATION OF NETTLESTONE AND NEWCHURCH PRIMARY SCHOOLS

# PRIVACY NOTICE FOR STAFF

### How We Use School Workforce Information

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

- Personal information (such as name, address, employee or teacher number, national insurance number).
- Special categories of data including characteristics information such as gender, age, ethnic group.
- Contract information (such as start dates, hours worked, post, roles and salary information).
- Work absence information (such as number of absences and reasons).
- Qualifications (and, where relevant, subjects taught).
- Medical information.
- Payroll information.

**Why we collect and use this information** - We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed.
- Inform the development of recruitment and retention policies.
- Enable individuals to be paid.

**The lawful basis on which we process this information** - We process this information under **the Education Act 1996.**

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

**Storing this information** - We hold school workforce data to comply with our legal obligations and to affect the contract.

**Who we share this information with -** We routinely share this information with our Local Authority (LA) and the Department for Education (DfE).

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

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

**Department for Education (DfE) -** We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy

Privacy Notice - Staff

THE FEDERATION OF NETTLESTONE AND NEWCHURCH PRIMARY SCHOOLS

monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

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

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

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

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

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

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

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

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

**Requesting access to your personal data** - Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the School Business Manager who is currently **Mr Mark Jacobs**.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress.
- Prevent processing for the purpose of direct marketing.
- Object to decisions being taken by automated means.

Privacy Notice - Staff

THE FEDERATION OF NETTLESTONE AND NEWCHURCH PRIMARY SCHOOLS

- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed.
- Claim compensation for damages caused by a breach of the Data Protection regulations.

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

**Further information** - If you would like to discuss anything in this privacy notice, please contact **Mr Mark Jacobs**, School Business Manager.

Privacy Notice - Staff