

THE FEDERATION OF NETTLESTONE & NEWCHURCH PRIMARY SCHOOLS



DATA PROTECTION POLICY

Date Agreed: March 2018

Review Date: March 2019

DMF Botlett

Signed: _____

Chairman Board of Governors

The Federation of Nettlestone & Newchurch Primary Schools

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

Revision No.	Date Issued	Prepared By	Approved	Comments
1	January 2018	DR	FGB	Formulation of Policy in line with model policy from ICO.
2	March 2018	KJH/H B/RP		Adaptions in light of Data Officer monitoring and changes required for the introduction of the General Data Protection Regulation 2018 (applicable from 25 th May 2018)
3	July 2018	KJH		GDPR Compliance

of the school community safe. We ensure that consistent effective safeguarding procedures are in place in order to support families, children and staff of the school.

Aims

Our Federation aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with all current data protection laws.

This policy applies to all personal data, regardless of format.

This policy ensures 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 risks of a data breach.

Legislation and guidance

This policy meets the requirements of the GDPR and is based on [guidance published by the Information Commissioner's Office](#) and [model privacy notices published by the Department for Education](#). It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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

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 <i>Set out in article 4(1) of the GDPR</i>
Sensitive personal data	Data such as: <ul style="list-style-type: none"> • 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
Processing	Obtaining, recording or holding data <i>Set out in article 4(2) of the GDPR</i>
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 <i>Set out in article 4(7) of the GDPR</i>
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller <i>Set out in article 4(8) of the GDPR</i>
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. <i>Set out in article 37-39 & 83 of the GDPR</i>

The data controller

The Federation of Nettlestone and Newchurch Primary School processes personal information relating to pupils, staff, visitors, suppliers and others, and therefore is a data controller. A data controller is responsible for complying with GDPR principles in an effective manner.

Each school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

The nominated individuals with overall responsibility for Data Protection are the Executive Headteacher and the Data Officer.

Roles and responsibilities

Everyone who works with the Federation of Nettlestone and Newchurch Primary Schools has some responsibility for ensuring data is collected, stored and handled appropriately.

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

Data Protection Officer

The Federation's Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. Currently the Local Authority provide this function on behalf of the Federation.

However, the following staff have additional key responsibilities:

- The Governing Body is ultimately responsible for ensuring the Federation of Nettlestone and Newchurch Primary School meets its legal obligations.
- The Executive Headteacher working alongside the nominated Governor responsible for monitoring Data Protection who is presently **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 or 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 and contracts or agreements with third parties that may handle the company's sensitive data
 - ✓ Ensuring all systems, services and equipment used for storing data meet 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 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:

All staff and volunteers are responsible for:

- ✓ Collecting, storing and processing any personal data in accordance with this policy.
- ✓ Informing the Federation of any changes to their personal data, such as change of address.
- ✓ Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
 - If they have concerns that this policy is not being followed.
 - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
 - If they need to rely on or capture consent, deal with protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
 - If there has been a data breach.
 - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
 - If they need help with any contracts or sharing personal data with third parties.

Data Protection Principles

The GDPR is based on data principles with which our Federation must comply.

The principles dictate that data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the Federation aims to comply with these principles.

Collecting Personal Data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' to do so under data protection law:

- 1) The data needs to be processed so that the Federation can fulfil a contract with the individual, or the individual has asked the Federation to take specific steps before entering into a contract e.g. employment contracts.
- 2) The data needs to be processed so that the Federation can comply with a legal obligation e.g. reporting to parents, reporting accidents, reporting exclusions etc

- 3) The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- 4) The data needs to be processed so that the Federation, as a public funded entity, can perform a task in the public interest and carry out its official functions.
- 5) The data needs to be processed for the legitimate reasons of the Federation or a third party (provided the individual's rights and freedoms are not overridden)
- 6) The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law in documents including the Privacy Notice.

The Federation processes the personal data of its employees, pupils, parents, Governors, suppliers, contractors etc so that it may manage the educational establishments in accordance with the law.

The Federation and each school processes the personal information of its pupils and their parents, to record their progress for statistical purposes and so at least an annual written report may be provided as required by law. For a child's protection, medical conditions and any other risk of harm will be documented. To meet with regulations the Federation may record behavioural standards and to record further information in the event of an accident or incident.

Annually, each school will contact each child/parent to gain permission to obtain and/or publish images when it is appropriate. In addition permission will be sought to take the child offsite for local trips/visits where prior notification has been given. If the school does not receive a reply it will consider no agreement has been given. Parents may withdraw consent at any point.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect data in documents such as the Privacy Notice.

The Federation will make it easy for data subjects to update the information that each school holds about them. For instance, via the new app - Parent Lite App from Capita.

If we want to use personal data for reasons than those given when we first obtained it, we will inform the individuals concerned before we do and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be actioned in accordance with the Records Management policy.

Sharing Personal Data

We will not usually share personal data with anyone else, but we may do where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies - we will seek consent as necessary before doing this, except in the case where it could compromise the protection and safeguarding of a child.
- Our suppliers or contractors need data to enable us to provide services to our staff/pupils e.g IT companies. When doing this we will:
 - Only appoint reputable suppliers or contractors which can provide sufficient guarantees that they comply with data law.
 - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and local authority or government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our pupils and staff.

Where we transfer personal data to a country outside the European Economic Area, we will do so in accordance with data protection law.

Subject Access Requests

Individuals have a right to make a subject access request to gain access to personal information that the Federation holds about them. Subject access requests must be submitted in writing and they should include:

- ✓ full name of individual
- ✓ contact address
- ✓ contact phone number and/or e:mail address
- ✓ details of the specific information required

Personal data about a child belongs to that child, and not the parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be able to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore most subject access requests from parents or carers of pupils within the Federation may be granted without the express permission of the pupil. This is not a rule and a pupils ability to understand their rights will always be judged on a case by case basis.

When responding to a subject access request we

- **will always** verify the identity of anyone making a subject access request before handing over any information.
- **will respond without delay and within one month of receipt of the request.**
- **will provide the information free of charge.**
- may inform the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

The Federation will provide any personal information that is held about an individual following the principles of the [ICO Subject Access Code of Practice](#).

We will not disclose it if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal a child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning a child.

Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we collect data regarding its use and lawful processing, individuals also have the right to:

- **Request correction** of their personal information. This enables the user 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 users 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.

Individuals are made aware of these rights when they join the Federation and should submit any request to exercise these rights to the DPO. If Federation staff receive such a request, they must immediately forward it to the DPO.

CCTV

We use CCTV within our Federation to ensure that the sites remain safe. We will adhere to the [ICO's code of practice](#) for the use of CCTV.

We do not need to ask individuals permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the use of CCTV should be directed to Ronni Petrossian.

Photographs and Videos

As part of our Federation and individual school activities, we may take photographs and record images of individuals within our setting.

We will obtain written consent from parents/carers for photographs and images to be taken of their child for communication, celebration, marketing and promotional materials as part of the admissions process.

Consent can be withdrawn or refused at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos we will not accompany them with any other personal information about the child, to ensure that they cannot be identified.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities including:

- Commissioning a suitably qualified DPO (the local authority currently oversee this role on behalf of the Federation)
- Only processing personal data that is necessary for each specific purpose of processing and always in line with data protection principles set out in relevant data protection law.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters.
- Conducting reviews and audits to test our privacy measures to ensure we remain compliant
- Maintaining records of our processing activities e.g. Privacy Notices, Data Audit

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper - based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on printers, on staffroom tables, pinned to notice/display boards or left anywhere where there is general access.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office.
- Data should be **protected by confidential strong passwords** that are changed regularly and never shared between employees - ideally 8 characters long and containing letters and numbers. Staff are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Wight Support can explain how to send data to authorised external contacts e.g. by password protection

- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.

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.

Questions about storing data safely should be directed to Wight Support or the School Business Manager.

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. Please see our Records Management Policy for more information on retention periods.

For example we will shred paper based records and overwrite or delete electronic files. We may also use a third party to safely dispose of documentation on the Federation's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal data breaches

The Federation will make all reasonable efforts to ensure that there are no personal data breaches.

In the unlikely event of a suspected breach, we will contact the DPO and follow their procedure as advised.

Training

All staff and governors have been provided with data protection training. Data protection training will be included as part of the induction training for all new staff who join the Federation as well as for existing staff to help them understand their responsibilities when handling data when required or requested.

Monitoring Arrangements

The Executive Headteacher, Governor Responsible for Data Protection and DPO are responsible for monitoring and reviewing this policy.

Links with other policies

This data protection policy and privacy notice is linked to the

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

PRIVACY NOTICE
for
THE FEDERATION OF NETTLESTONE AND
NEWCHURCH PRIMARY SCHOOL

Privacy Notice: How we use pupil information

This school is a member of the Federation of Nettlestone & Newchurch Primary School 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 Regulation 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; and
- 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 is in compliance with the Data 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:

For the DfE:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

PRIVACY NOTICE
for
THE FEDERATION OF NETTLESTONE AND
NEWCHURCH PRIMARY SCHOOL

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 effect the contract.

Who we share this information with

We routinely share this information with:

- our local authority
- 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 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; and
- 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 **Ms Ronni Petrossian**

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
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 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 **Ms Ronni Petrossian**, School Business Manager.

Appendix c - When and How to Share Information

