Wellingborough
Nursery Schools Federation

General Data Protection Policy Sept 2020

Introduction:

WNSF is committed to ensuring that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with its legal and regulatory obligations.

This policy sets out the expected behaviours of employees in relation to the collection, use, retention, transfer, disclosure and destruction of personal data belonging to data subjects.

The Federation's leadership and Governors are fully committed to ensuring continued and effective implementation of this policy and expects all staff to share in this commitment. Any breach of this policy will be taken seriously.

The policy is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education. It also takes into account the requirements of the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018, as set out in the Data Protection Bill.

Scope:

This policy applies to all individuals where a data subject's personal data is processed.

The Federation processes personal information to enable us to provide education, training, welfare and educational support services, to administer school property, and to support and manage our employees.

The policy applies to all processing of personal data in electronic form, including email and documents created with word processing software, or where it is held in manual files that allows ready access to information about individuals.

We also use CCTV for security and the prevention and detection of crime. The policy reflects the ICO's code of practice for use of surveillance cameras and personal information.

Accountability and governance

This policy applies to all staff employed by the Federation, and to external organisations or individuals working on the Federation's behalf. Staff who do not comply with this policy may face disciplinary action.

The governing body of the Federation has overall responsibility for ensuring that the Federation complies with all relevant data protection obligations.

WNSF processes personal information relating to pupils, staff, parents and visitors and, therefore, is defined as a Data Controller. The Schools are registered as a Data Controller with the Information Commissioner's Office and renews its registration annually.

Article 5(2) of the GDPR also requires that…"the controller shall be responsible for, and be able to demonstrate, compliance with the principles." The Principal acts as the representative of the data controller on a day-to-day basis.

The Federation has appointed a Data Protection Officer who is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities directly to the governing body and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPO can be contacted at **bursar@croyland-nur.northants-ecl.gov.uk or bursar@highfeld-nur.northants-ecl.gov.uk**, or by writing to: The data Protection officer is Lyndsey Barnett

Croyland Nursery School
Croyland Road
Wellingborough
NN8 2AX

Highfield Nursery School
Finedon Road
Wellingborough NN8 4AB

Data Protection principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the 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 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.

Lawful basis for processing

5.1 In accordance with the GDPR the Federation must have a valid lawful basis in order to process personal data and special category data.
5.2 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the Federation processes personal data:

(a) **Consent:** the individual has given clear consent for the Federation to process their personal data for a specific purpose.
(b) **Contract:** the processing is necessary for a contract the Federation has with the individual, or because they have asked the Federation to take specific steps before entering into a contract.
(c) **Legal obligation:** the processing is necessary for the Federation to comply with the law (not including contractual obligations).
(d) **Vital interests:** the processing is necessary to protect someone's life.
(e) **Public task:** the processing is necessary for the Federation to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
(f) **Legitimate interests:** the processing is necessary for the Federation's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform its official tasks.)

5.3 The Federation has informed people about the lawful basis for processing their personal data and these are now included in its privacy notices.

The rights of data subjects

6.1 The GDPR and the DPA 2018 provides the following rights for individuals:

- The right to be informed
- The right of access
- The right of rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

6.2 The Federation ensures that procedures are in place to enable the efficient processing of data subjects' rights:

- Fair processing information is provided through the Privacy Notices published on the Federation's website;

- Retrieval and verification of personal data and supplementary information is permitted through the Subject Access Request (SAR) process (see Appendix A);
- Should personal data or information be found to be inaccurate or incomplete the Federation will resolve this as appropriate, where a SAR request for rectification is submitted to the Data Protection Officer;
- The Federation will not apply the right to erase where personal data is processed lawfully to comply with a legal obligation for the performance of a public task or exercise of its official authority;
- The processing of personal data will be restricted through the submission of a SAR where the accuracy of data is contested; where an individual objects to the processing; when processing is deemed as unlawful; or where information is no
- longer needed but the personal data is required by an individual to establish, exercise or defend a legal claim;
- When responding to a SAR the Federation will provide personal data to a subject in a structured, commonly used and machine readable form (subject to technical compatibility), and it will be provided free of charge;
- Where an objection to data processing is raised the Federation will stop processing the personal data unless there are compelling legitimate grounds for the processing that override the data subject's right. Individuals will be informed of their right to object at the point of first communication. This is published in the Federation's Privacy Notices;

Data security

7.1 The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.
7.2 The Federation fully recognises its responsibilities to protect personal information that staff collect and use, including requirements to prevent personal data being accidentally or deliberately compromised. The Federation adopts physical, technical and organisational measures to ensure the security of personal data.

Sharing of Information with Third Parties:

There may be circumstances where the school is required either by law or in the best interests of students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities have to adhere to data protection law and have their own policies relating to the protection of any data that they receive or collect. Personal data about children, will not be disclosed to third parties without the consent of the child (at an age who can act for themselves, specified under GDPR guidance) the child's parent or carer, unless it is obliged by law or in the best interest of the child.

Examples of data that may be disclosed to third parties without the need for consent:
• Other schools If a pupil transfers from one school to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school.

• Health authorities (under health legislation), the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• Police and courts If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation.

• Social workers and support agencies In order to protect or maintain the welfare of pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• Department for Education and Ofsted to help the government monitor and audit school performance and enforce laws relating to education.

The intention to share data relating to individuals to an organisation outside of the school shall be clearly defined within notifications and details of the basis for sharing given. These details are provided in the 'Information Audit Document' located on the school website. Data will be

shared with external parties in circumstances where it is a legal requirement to provide such information, or where it is for the purpose of pupil provision, such as school meals and on-line curriculum work.

Any proposed change to the processing of individual's data shall be notified to them (see the 'Information Audit Document' above). Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure ***would not*** be in the best interests of the child
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed.

General staff guidelines

7.3.1 The only people able to access data covered by this policy are those who need it for their work.
7.3.2 Data should not be shared informally. When access to confidential information is required, staff should request it from appropriate managers.
7.3.3 The Federation will provide training to all staff and governors to help them understand their responsibilities when handling data.
7.3.4 Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
7.3.5 In particular, strong passwords must be used and they should never be shared.
7.3.6 Personal data should not be disclosed to unauthorised people, either within the Federation or externally.
7.3.7 Data should be regularly reviewed and updated if it is found to be out of date. If no longer required is should be deleted and disposed of appropriately.
7.3.8 Staff should seek guidance from managers or the Data Protection Officer if they are unsure about any aspect of data protection.

Data storage

7.4.1 When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.
7.4.2 These guidelines apply to data that is usually stored electronically but has been printed out for operational purposes:

- When not required the paper or files should be kept in a locked drawer or filing cabinet;

- Staff should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or copier;
- Data printouts should be shredded and disposed of securely when no longer required

7.4.3 When data is stored electronically it must be protected from unauthorised assess, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees;
- If data is stored on removable media these should be kept locked away securely when not being used;
- Data should only be stored on designated drives and servers, and should only be uploaded to approved 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 IT managed service 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.

7.4.4 The IT managed service will ensure that all systems, services, software and equipment meet acceptable security standards

Data use:

5.1 Personal data is at greatest risk of loss, corruption or theft when it is accessed and used. When working with personal data staff should ensure that:

- The screens of computers are always locked when unattended;
- Data must be encrypted if being transferred or stored electronically;
- Data should not be saved to staff's own computers, devices, or personal email addresses.

Data accuracy

7.6.1 The law requires the Federation to take reasonable steps to ensure that data is kept accurate and up to date. It is the responsibility of all staff who work with data to take practical measures to ensure it is kept as accurate and up to date as possible.

7.6.2 Data will be held in definitive staff or pupil personal files. Staff should not create any unnecessary additional data sets, or files relating to pupils and staff.

Data breaches

7.7.1 The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. In the UK the supervisory authority is the Information Commissioner's Office (ICO).
7.7.2 The Federation must inform the ICO of any breach within 72 hours of becoming aware of that breach, where feasible.
7.7.3 All members of staff have an obligation to report actual or potential data protection compliance failures to the Data Protection Officer without delay.
7.7.4 The Data Protection Officer will investigate the reported breach in order to determine whether or not the ICO and affected individuals need to be notified.
7.7.5 A register of personal data breaches will be maintained, regardless of whether these have been notified or not.

Data retention

9.1 In accordance with GDPR principles and to ensure fair processing the Federation will not retain personal data for longer than necessary in relation to the purpose for which it was originally collected, or for which it was further processed.
9.2 All personal data will be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need for it to be retained.

Wellingborough
Nursery Schools Federation

SUBJECT ACCESS REQUEST (SAR)

Please complete this form is you wish to exercise your rights in relation to:
 Getting access to your personal information;
 Raising an objection or restricting your data processing;
 Rectifying or erasing information that you think is incorrect or unlawful;

When you have completed the form please print, sign and send to the relevant school
In order for the Federation to release or amend any personal data, and to protect your confidentiality you will need to supply proof of identity. Acceptable evidence is an official identity document containing a photograph, such as a current driving license or passport. Please bring your ID to the school reception for verification.

Details of the person making the request:

Title:
First name(s):
Last name:

Date of birth:
Address:
Telephone:
Email:

Describe the information you are requesting, or whether you wish to raise an objection, restriction, erasure, or rectification.

Please be as specific as possible and include all relevant detail about your request and about what exact information you wish to access or verify. Please note if insufficient detail is provided, we may have to come back to you to seek clarification.

Declaration: I certify the information on this form is true and correct

Sign:
Date:

If as a result of your request you are dissatisfied with the way the Federation is using your personal data you should raise this matter with the Data Protection Officer at the address provided above. We will do everything we can to put matters right and if we disagree with you we will tell you our reasons.

Policy reviewed Sept 2020