The Federation of Duke Street and Highfield Nursery Schools

Data Protection Policy

Policy Leader / DSL / EHT*	**Susan Conron, Executive Headteacher and DSL**
Last Updated by School	**September 24**
Communicated to staff:	Annual updates 24/09/24
Review period	Annually
Approved by the Governing Body	*Future date 14/10/24*

Policy 2. Data Protection Policy

The following policy relates to all Federation of Duke Street and Highfield Nursery School employees (including voluntary, temporary, contract and seconded employees), who capture, create, store, use, share and dispose of information on behalf of Federation of Duke Street and Highfield Nursery School.

These persons shall be referred to as 'Users' throughout the rest of this policy.

Federation of Duke Street and Highfield Nursery School shall be referred to as 'the school' or 'we' throughout the rest of this policy.

The following policy relates to all electronic and paper based information.

"Think about the minimum amount of data required to achieve your goal, you should only see the data you need to see".

Supporting documentation:

https://www.gov.uk/guidance/data-protection-in-schools

Dfe GDPR toolkit for schools

Statement of Commitment

In order to undertake our statutory obligations effectively, deliver services and meet customer requirements, the school needs to collect, use and retain information, much of which is personal, sensitive or confidential.

Such information may be about:

- Pupils.
- Parents and Guardians.
- Governors.
- Employees or their families.
- Members of the public.
- Business partners.
- Local authorities or public bodies.

We regard the lawful and correct treatment of personal data by the school as very important to maintain the confidence of our stakeholders and to operate successfully.

To this end, the school will ensure compliance, in all its functions, with the Data Protection Act (DPA) 1998, the General Data Protection Regulation (GDPR) and the new Data Protection Act (DPA) 2018, and with other relevant legislation.

Data Protection Principles

The Principles of DPA and GDPR state that personal information must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals; the lawful basis can be:

    - Consent of a data subject
    - Processing is necessary for the performance of a contract with the data subject
    - Processing is necessary for compliance with a legal obligation (e.g. The Education Act 1996, School Standards and Framework Act 1998, Education Act 2002, Children and Families Act 2014)
    - Processing is necessary to protect the vital interests of the data subject or another person (e.g. life or death)
    - Processing is necessary for the performance of a task carried out in the public interest

    The lawful basis for sensitive personal data (racial, political, religious, trade union, genetic, health, sex life, criminal convictions or offences) is:

    - Explicit consent of the data subject
    - Processing is necessary for carrying out obligations under employment, social security or social protection law
    - Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent
    - Processing relates to personal data manifestly made public by the data subject
    - Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Processing is necessary for reasons of substantial public interest
    - Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the

employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. Accurate and, where necessary, kept up to date

5. 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

6. Processed in a manner that ensures appropriate security of the personal data against unauthorised processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Compliance with the Data Protection Principles and Data Protection Legislation

In order to comply with these principles and meet all data protection obligations as stipulated in data protection legislation, the school will:

- Raise awareness of data protection across the school.
- Offer data protection training to all employees and governors.
- Create a data protection policy for the school that is updated annually.
- Complete a personal data processing audit, which lists the following:
    - Name of the personal data set.
    - Purpose for processing this personal data set.
    - Who the data set is shared with.
    - Is the data transferred to another country.
    - How long do you keep the personal data set (retention).
    - The technical and organisational security measures to protect the personal data set.
    - The legal basis for processing as described above (1).
    - If consent is the legal basis for processing, details of the evidence of this consent.

- Put any risks found from the personal data processing audit process into a risk register.
- Review the school's consent forms so they meet the higher standards of GDPR, create an audit trail showing evidence of consent.
- Under 13's can never themselves consent to the processing of their personal data in relation to online services, this rule is subject to certain exceptions such as counselling services.
- Register with the Information Commissioners Officer as a data controller.
- Appoint a data protection officer who will monitor compliance with the GDPR and other data protection laws.
- Create a privacy notice that will let individuals know who we are, why we are processing their data and if we share their data.
- Create a system to allow data subjects to exercise their rights:
    - Right to be informed via a privacy notice.
    - Right of access via a subject access request within 1 month.
    - Right of rectification to incorrect data within 1 month.
    - Right to erasure unless there is a legal reason for processing their data.
    - Right to restrict processing to the bare minimum.
    - Right to data portability to receive their data in the format they request.
    - Right to object to personal data being used for profiling, direct marketing or research purposes.
    - Rights in relation to automated decision making and profiling.
- Amend any business contracts with suppliers to ensure that they will conform to new data protection legislation.
- Implement technical and organisational controls to keep personal data secure.
- Use Privacy Impact Assessments to assess the privacy aspects of any projects or systems processing personal data.
- Ensure an adequate level of protection for any personal data processed by others on behalf of the school that is transferred outside the European Economic Area.
- Investigate all information security breaches, and if reportable, report to the Information Commissioners Office within 72 hours.
- Undertake data quality checks to ensure personal data is accurate and up to date.
- Demonstrate our compliance in an accountable manner through audits, spot checks, accreditations and performance checks.
- Support the pseudonymisation and encryption of personal data.

Management & Monitoring of Electronic Communications

Introduction
These guidelines have been developed to provide information about electronic communications best practice,and will hopefully help you balance staff and student privacy with the oversight necessary to ensure your safeguarding obligations are maintained.

The sections are:

- E-mail
- Messaging and Discussion Tools
- Monitoring staff and student use
- Essential Resources (including relevant legislation)
- What you need to know about Social Media

All electronic communications, whilst they are held, are disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an e-mail, an Instant Message (IM), a text, or on a message board, could potentially be made public. Electronic communications are very easy to copy and transmit and although you may have deleted your copy the recipients may not. Because of this they can form part of your records, commit you to contracts and expose your school to risk if used badly.

E-mail
Watch your language
As communicating by e-mail is quick and easy, the language in which e-mail is written is often less formal and more open to misinterpretation. Use spell-check and consider the tone of your wording.

Ensure that Bcc is used where appropriate to avoid the unauthorised disclosure of e-mail addresses of intended recipients. The ICO has taken enforcement action in cases where Bcc has not been used in sensitive cases.

Secure your data
The consequences of an e-mail containing sensitive information being sent to an unauthorised person can result in a fine of up to 20 million euros (or equivalent in sterling) or restrictions on processing from the Information Commissioner, along with adverse publicity for your school. Confidential or sensitive information should be sent by a secure encrypted e-mail or data transfer system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

Secure your devices
Did you know that e-mail Apps on mobile phones are usually unprotected? Did you know that, by default, Outlook will download the entire contents of a person's mailbox on a personal device (which can be easily accessed)?

If members of staff access school e-mails on personal devices, the school's IT support provider should be contacted for help with configuring the device and check for encryption, as well as ensuring that all devices require a suitable password for access. The key is to engage with your IT support provider who will be able to advise accordingly.

You could advise staff to only access work e-mail via the internet as the web client does not save data locally.

How long do we keep emails?

Email is a communication tool, and e-mail applications are not designed for keeping e-mail as a record. E-mail that needs to be kept should be identified by content, for example:
-Does it form part of a pupil record?
-Is it part of a contract?
-Does it relate to an employee?

Information contained within these e-mails should be recorded in the appropriate place (e.g. the MIS or behaviour management system). Once this is done the original could be deleted.

Consider implementing an electronic rule whereby emails in inboxes are automatically deleted after a period of time.

This will assist greatly in reducing the amount of information potentially disclosable in the event that a subject access request is received.

Limiting the information which is retained will mitigate the school's liability in the event of a breach and will reduce the amount of electronic storage required.

Physical security

Physical access to records should be restricted. Key IT Infrastructure, servers, certain desktop/laptop devices and paper records must be kept in restricted environments, or areas with controlled access. Staff code of conduct, online safety policy and safeguarding policy are reviewed and updated annually.
Whilst the removal of hard copy documents is not encouraged there are occasions when it is necessary and in this instance, staff should consult the Data Protection policy and other mentioned policies for guidance on best practice in this instance.
Any security breaches involving physical security of data must be reported to the Data Protection Officer in either school who will report to ICO if the breach will affect/cause damage to the individual whom the data belongs to.

In the event of a data breach, the Data Protection Officer is informed promptly and will escalate to the ICO who will further advise of next steps.
It is the responsibility of the DPO to update and liaise with the ICO and keep the SIRO fully updated of the data breach and the ongoing situation.

Sharepoint – Autumn 2024

Autumn 2024: to optimise efficiency across the federation, sharepoint is in the process of being finalised. Natalie Sinclair, Head of School Highfield is the owner and author of sharepoint. Depending on nature of data, folders and documents are restricted due to sensitive information.

Sharepoint is backed up under the SLA with Education Digital services.

A3 and A1 licences and multifactor authenticator in use.

Rights of the Individual

The list of rights that a data subject (person who the data is about) can exercise has been widened by Section 2 of the GDPR:

- The right to be informed; via privacy notices.
- The right of access; via subject access requests (SARS), the timescale for response has been reduced from 40 calendar days to one calendar month.

SARs must be free of charge, charges can only be made for further copies or where requests for information are unfounded or excessive.

- The right of rectification; inaccurate or incomplete data must be rectified within one month.
- The right to erasure; individuals have a right to have their personal data erased and to prevent processing unless we have a legal obligation to do so.
- The right to restrict processing; individuals have the right to suppress processing. We can retain just enough information about the individual to ensure that the restriction is respected in future.
- The right to data portability; we need to provide individuals with their personal data in a structured, commonly used, machine readable form when asked.
- The right to object; individuals can object to their personal data being used for profiling, direct marketing or research purposes.
- Rights in relation to automated decision making and profiling; GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

The school will ensure that these rights will be exercised.

Contact

SIRO (Senior Information Risk Owner) & Data Protection Controller:
Susan Conron
head@dukestreet-nur.lancs.sch.uk
01257262430

Contact the Data Protection Officer by:

Email: bursar@dukestreet-nur.lancs.sch.uk or bursar@highfield-nur.lancs.sch.uk

Phone: 01257262430 or 01257262556

Post: Duke Street Nursery School, Duke Street, Chorley, PR7 3DU
Highfield Nursery School, Wright Street, Chorley PR6 0SL