Dale Community Primary and Stonehill Nursery Federation

Data Protection Policy

Head Teacher: **Louise Foster**

Chair of Governors: **Diane Williams**

Policy Approved by: **Governors Finance and Personnel Committee**

Policy reviewed by:	Governors Finance and Personnel Committee	Date: 18 October 2016
Policy reviewed by:	Governors Finance and Personnel Committee	Date: 26 June 2018
Policy reviewed by:	Governors Finance and Personnel Committee	Date: 23 June 2020
Policy reviewed by:	Governors Finance and Personnel Committee	Date:

DATA PROTECTION

Dale and Stonehill are committed to providing a secure environment in which we fully protect the data that we hold and store. As staff and governors, we have both statutory and personal responsibilities to do this. This policy, along with our Privacy Notices, will set out clearly how we use and protect data. Other documents referenced in this policy can be found at www.dale.derby.sch.uk/gdpr

If you would like more information about this, or any other school policy, please do not hesitate to contact the school office on admin@dale.derby.sch.uk

The General Data Protection Regulation (GDPR) is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. Both exist to protect an individual's 'data' and school must demonstrate that they are acting within the law and adhering to the principals of both.

'Data' is referred to many times in the policy and describes, "any information that relates to a living person that can identify them'. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions. Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

We are required to collect sensitive data for the Department of Education and Local Authority requirements. Pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be required. We must have a legitimate reason to hold the data we collect. These reason(s) are explained in more detail in our Privacy Notices, found on the school website. We will often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are some circumstances you cannot withdraw consent; these are explained in 'Data Subject Rights' section below.

Data Collection and Accuracy

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection. We will only collect the minimum amount of data needed for a particular task or reason. If there is a breach, there will be processes in place to ensure that only limited information can be lost.

Data collected must be accurate, and steps are taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis. Teachers and Teaching Assistants take time to go through the Pupil Admission Form with parents and carers, to ensure they understand what types of data are being collected and how it will be used.

If you feel that any data, we are holding, is inaccurate, you can request that it is amended or removed; you must complete a 'Withdrawal Consent Form' to do this. There is also a complaint procedure to follow if you feel your request has not been handled correctly. Please see the GDPR section of the school website.

Data Retention
Our Retention Policy document explains how long we store records for and how we dispose of it.

Data Security
Our Confidentiality Policy, CCTV Policy and ICT Acceptable Use Policy, along with our Privacy Notices, all outline processes we use to keep data safe. Our Staff Handbook, issued to all the school workforce, explains individual responsibilities for keeping data safe, whether that be paper files, electronic records or other information. The handbook is revisited annually, along with staff training to ensure data security is achieved.

Data Subjects'
A 'data subject' is anyone whose personal data we hold. A data subject has the right to:

- Be informed of the data that is held about them or their children
- Access data stored about them or their children
- Amend any error(s) on the data stored
- Remove data if there is no longer a need for school to keep it
- Restrict processing and limit what is done with their data
- Object to data being shared or collected.

These rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

Subject Access Requests
You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You need to fill out an 'SAR Request Form' and will need to provide identification evidence for us to process the request.

We are required to provide the data requested within one month, but this can be extended in some circumstances if, for example, the school was closed for holidays. The maximum extension is up to two months. When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query. In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. school nurses who are employed by the NHS.

We will supply the information in an electronic form. If you wish to complain about the process, please see our complaints procedure.

Data Controllers and Processors
Our School Governors are our 'Data Controllers'. They have ultimate responsibility for how school manages data. They delegate this to Data Processors to act on their behalf.

The Data Controller can be any member of the staff workforce that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected.

Data may also be processed by a third-party company, a contractor, a temporary employee or an organisation such as the police or the Local Authority.

Staff are given training to ensure they are handling data correctly and we have contractual agreements in place to ensure third-party organisations are obliged to do the same.

Processing Data
We must always have a reason to process data about an individual. Our Privacy Notices set out how we use data in more detail. GDPR outlines six conditions for lawful processing and any time we process data relating to an individual, it is within one of those conditions. If there is a 'data breach', we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:

- Consent obtained from the data subject or their parent
- Performance of a contract where the data subject is a party
- Compliance with a legal obligation
- To protect the vital interests of the data subject or other associated person
- To carry out the processing that is in the public interest and/or official authority
- It is necessary for the legitimate interests of the data controller or third party
- In accordance with national law.

In addition, any special categories of personal data are processed on the grounds of:

- Explicit consent from the data subject or about their child
- Necessary to comply with employment rights or obligations
- Protection of the vital interests of the data subject or associated person
- Being necessary to comply with the legitimate activities of the school
- Existing data that has been made public by the subject and is no longer confidential
- Bringing or defending legal claims
- Safeguarding
- National laws in terms of processing genetic, biometric or health data.

Data Sharing
We only share data within the limits set by GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared. Decisions taken whether to share or not share data are made by our School Governors, Senior Leadership Team and are recorded in school.

Breaches and Non-compliance
If there is non-compliance with the policy or processes, or there is a 'data breach' (as described within the GDPR and DPA 2018 regulations) then we follow our *Breach and* Compliance Procedure. Protecting data and maintaining data subjects' rights is the purpose of this policy and full details can be found on the school website.

Consent
As a school we seek consent from the staff workforce, volunteers, young people, parents and carers, so that we may collect and process an individual's data. We are clear about our reasons for requesting the data and how we use it. There are contractual, statutory and regulatory occasions when consent is not required. In most cases data will only be processed if explicit consent has been obtained. In some cases, we may seek consent directly from the young person, but this will be dependent on the child and the reason for processing.

Consent and Renewal
On the school website, we have Privacy Notices that explain how data is collected and used for each data subject. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important. We want to ensure the accuracy of that information gathered and adhere to our retention policies, for disposal of data that is no longer required.

For Pupils, Parents and Carers
On arrival at school, you will be asked to complete an 'Admissions Form' giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes. If you require any support to complete this form a member of staff will be happy to help you. We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. Please see the 'Data Collection' section above for more information about this.

Pupil Consent Procedure
Where processing relates to a child under 16 years old, we will obtain the consent from a person who has parental responsibility for the child. A Pupil may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent
Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles. Please complete the 'Consent Withdrawal Form' to action this.

CCTV and IT Security
We use CCTV and store images in line with the policy. CCTV may be used for:

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behavior and exclusion management processes
- To assist the school in complying with legal and regulatory obligations.

For more information please read our CCTV Policy, found on the school website.

Data Protection Officer
Our Data Protection Officer, John Walker, has responsibility to:

- Inform and advise the Data Controllers and Processors of their obligations under GDPR
- Monitor compliance with the GDPR and DPA
- Give advice about the data protection impact assessment and monitor its performance
- Be the point of contact for Data Subjects if there are concerns about GDPR
- Cooperate with the supervisory authority and manage the breach procedure
- Advise about training and CPD for the GDPR.

You can contact him by email: john@jawalker.co.uk

Physical Security
In school, every secure area has individuals who are responsible for ensuring that the space is maintained and controlled. Offices and cupboards, that contain personal data, are locked if the processor is not present.

Our Site Manager is responsible for authorising access to secure areas along with our Senior Leadership Team.

All Staff, contractors and third parties who have control over lockable areas are required to take due care to prevent data breaches.

Secure Disposal
We have processes in place to dispose of data securely. Our IT Manager is responsible for ensuring that all hardware is disposed of as per GDPR requirements.

Our School Business Manager and Administrative team, along with the Senior Leaders are responsible for following Retention Policies when disposing of any data.

All data sensitive documents are shredded using our GDPR compliant shredder.

Complaints & the Information Commissioner Office (ICO)
Our Complaints Policy deals with complaints, including those relating to Data protection issues. You have a right to complain if you feel that data has been shared without consent or lawful authority. You may also complain if you have asked to us to erase, rectify or refrain from processing data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure if this is not successful. Please follow our GDPR Complaints Procedure, found on the school website. If you continue to be dissatisfied and wish to take a complaint further, please see below for more information.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk.

Review
The Data Protection Officer will conduct a review of the effectiveness of GDPR compliance and processes every 24 months.