Dinglewell Junior School
Data Protection Policy
Written by: Helen Howe, February 2018
Reviewed: February 2023
Next Review: February 2025

Dinglewell Junior School is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

"We have carefully considered & analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the public sector equality duty requirement to have due regard to the need to eliminate discrimination, advance equality or opportunity and foster good relations."

1. Aims

Dinglewell Junior School aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulations May 2018. This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the General Data Protection Regulations as published by the Information Commissioner's Office.

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.

3. 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
Sensitive personal data	Data such as: 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
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
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller
Data Protection Officer	A data protection officer (DPO) is a role required by the General Data Protection Regulation (GDPR). Data protection officers

	are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the School Business Manager. The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The General Data Protection Regulations 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 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

6. Role and Responsibilities

- The governing board has overall responsibility for ensuring that the school complies with its obligations under the General Data Protection Regulation 2018
- Day-to-day responsibilities rest with the School Business Manager or the Head Teacher in the School Business Manager's absence. The School Business Manager will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.
- Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7. Privacy/fair processing notice

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions
- We will only retain the data we collect for as long as is necessary, following DfE and Local Authority guidelines, to satisfy the purpose for which it has been collected.
- We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.
- We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures
- We will only retain the data we collect for as long as is necessary, currently 12 years, following DfE and Local Authority guidelines, to satisfy the purpose for which it has been collected.
- We will not share information about staff with third parties without consent unless the law allows us to.
- We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.
- Any staff member wishing to see a copy of information about them that the school holds should contact the School Business Manager, Data Controller.

Risk Assessments
Information risk assessments will be carried out by the Data Controller to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Impact Levels and protective marking
The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual and digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated, the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students/pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer, e.g

"When you have finished with it, this document should be added to one of the secure storage facilities for confidential information for destruction; these are located in the data office and Reception."

Audit Logging/Reporting/Incident Handling
Audit logs will be kept to provide evidence of accidental or deliberate data security breaches - including loss of protected data or breaches of an acceptable use policy, for example. All incidents will be logged with the Network Manager. Our current technical partner for audit logging is South West Grid for Learning.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a 'responsible person' for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

Subject access requests
Under the General Data Protection Regulations 2018, pupils have the right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The pupil's name
- A correspondence address
- A contact number an email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

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

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably use secure remote access to school systems;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location. Data retrieved via dropbox must only be accessed on school hardware to ensure the encryption levels are in place.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and

Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly, i.e. a minimum of 8 characters and containing at least one upper case character, one number and one 'other' character e.g. -, /, & etc. User passwords must never be shared. Personal data may only be accessed on machines that are securely password protected.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for storage of personal data.
When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data /device must be encrypted and password protected,
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

We have clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems including off-site backups.
We have clear policy and procedures for the use of 'Cloud Based Storage Systems' (for example Dropbox, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.
As a Data Controller, Dinglewell Junior School is responsible for the security of any data passed to a 'third party'. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
All papers based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site with the exception of school trips where the material is the responsibility of the trip leader. We recognise that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (see Freedom of Information Act 2000 Policy) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Parental requests to see the educational record
Parents have the right of access to their child's educational record, free of charge, within 15 school days of a request.

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access rights.
For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.
The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at our school may be granted without the express permission of the pupil.
If parents ask for copies of information, they will be required to pay the cost of making the copies.

Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office.
- Passwords that are at least 8 characters long containing letter and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils 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.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. This retention/destruction of personal data and confidential school information will comply with the Retention Guidelines document provided for schools by the Information and Records Management Society.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated or be disposed of through an approved third party.

Documents for destruction by an approved third party will be added to one of the secure storage facilities for confidential information for destruction. These storage facilities will be emptied by either the Site Manager or Deputy Site Manager and disposed of through that approved third party; certificates of secure destruction will be trained by the School Business Manager.

It is recognised that the Site Manager will have contact with confidential personal/organisational material, etc in the course of their duties. It is the Site Manager's

responsibility to ensure that the emptying of secure disposal storage is restricted to the him/herself with the understanding that contents of such files must be kept confidential; Site Manager job description reflect this requirement.

Training

Our staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where annual training and any changes to legislation or the school's processes make it necessary.

This document will be reviewed once the General Data Protection Regulation comes into force, and then every 2 years. At every review, the policy will be shared with the Governing Board.

Appendix 1 – Use of technologies and Protective Marking

Government Protective Marking Scheme label	Impact Level (IL)	Applies to school?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	**May apply in Dinglewell Junior School e.g. some meeting minutes**
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	Will not apply in schools

Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, e.g the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The following from the SWGfL provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils' work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil/student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil/student record available in this way.