WINDHILL PRIMARY SCHOOL

FLYING HIGH FOR EXCELLENCE

Data Protection Policy

Person responsible for policy:	Donna Howard
Approved by:	School Leadership Team
Approval date:	September 2025
Review date:	September 2026

Ofsted Good Provider

Bronze Eco-Schools Bronze Award

Artsmark Silver Award Awarded by Arts Council England

Healthy School

School Games Gold 2022/23

Version:	2.0
Author:	School Data Protection Officer
Approved by:	School Leadership Team
Date approved:	
Review date:	September 2025
Target audience:	All Staff/Pupils/Citizens

Contents

1. Summary

This policy sets out how the school will comply with data protection legislation and protect the personal information of everyone who receives services from, or provides services to, the school. It informs individuals of their rights, and suppliers of their responsibilities. It shows how we comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, other regulations and good practice standards.

2. Scope

This policy applies to staff, contractors, agency staff and Governors. It covers personal data we collect and use on paper and electronically. It covers our databases, computer network and archive of paper records. It covers video and photographs, voice recordings, CCTV and mobile devices such as laptops, iPads, mobile phones and memory sticks.

3. Accountability

The *School* is a data controller which means that it decides why and how personal data is processed. It is accountable for its handling of personal information.

Our *School Leadership Team* is accountable for providing the policies for employees to follow under the law, so that we can respond to our statutory functions. The Data Protection Policy is part of our governance framework, which contains important policies and procedures maintained and published by the school, that are key to good governance and effective decision making.

The *Senior Information Risk Officer* (SIRO) is the Head Teacher who is accountable for protecting the school's information assets.

The *Data Protection Officer* is a position required in law to ensure the school complies with data protection legislation and acts as a single point of contact for individuals who want to exercise their rights under Chapter 3 of the UK GDPR. (See also section 23)

Each *employee and supplier* is bound by a contractual duty of confidentiality.

The school is registered with the *Information Commissioner*, who is the independent regulator appointed to check compliance with data protection law.

The school maintains a *register of processing activities* of the personal information we are responsible for to ensure it is used according to the data protection principles.

4. Data protection is a fundamental right

The protection of a person's personal and special category data is a fundamental right. Under the Human Rights Act 1998, everyone has the right to respect for their

private and family life, their home and their correspondence. This includes respect for your private and confidential information, particularly when storing and sharing data.

This right can be limited in certain circumstances but any limitation must balance the competing interests of an individual and of the community as a whole.

In particular any limitation must be covered by law and be necessary and proportionate for one or more of the following aims:

- public safety or the country's economic wellbeing
- prevention of disorder or crime
- protecting health or morals
- protecting other people's rights and freedoms
- national security.

The right to privacy must often be balanced against the right to free expression.

5. Personal data

In this policy we use the terms “personal data” and “special categories of personal data” which are used in data protection legislation.

In this policy personal data means any information relating to an identifiable living person. This means they can be identified from information such as a name, an address, an identification number (e.g. your National Insurance number, NHS number or case reference number), location data, financial data, etc.

“Special categories of personal data” is personal sensitive data. This is data regarding an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.) for the purpose of uniquely identifying a person, data concerning health or data concerning a person’s sex life or sexual orientation.

There are extra safeguards for special categories of personal data to ensure no one is discriminated against when it comes to receiving a service.

We generally refer to a person or individual in this policy, although the term in law is “data subject”.

The frequent reference in this policy to “processing” data means any operation performed on personal data, whether using a computer or manual filing systems. It includes collection, use, and recording, storing, sending and deleting personal data.

6. Data protection principles

The school applies data protection principles in its processing of personal data. These principles are set out in the UK GDPR and have been incorporated into the Data Protection Act 2018. The six principles are that personal data should be:

- Processed lawfully, fairly and in a transparent way
- Collected for a specific purpose
- Adequate, relevant and limited to what's necessary
- Kept up to date
- Kept for only as long as necessary
- Protected with appropriate security.

7. Lawful basis of processing personal data

There are different lawful reasons for processing personal data and special categories of personal data. The school always uses at least one lawful basis for processing personal information and at least one lawful basis for processing special categories of personal data.

The six lawful reasons for processing personal data are:

a) An individual has given consent for the processing of his or her personal data, and it is freely given, specific, informed, and there must be an indication signifying agreement;

b) the school has a contract with a person or organisation and needs to process personal data to comply with our obligations under the contract; or we haven't yet got a contract with the person, but they have asked us to do something as a first step (e.g. provide a quote) and we need to process their personal data to do what they ask;

c) The school is obliged to process personal data to comply with the law. We will always refer to the specific legal provision or source of advice that explains generally applicable legal obligations;

d) The processing of personal data is necessary to protect someone's life ("vital interests");

e) The processing of personal data is necessary under public functions and powers set out in law; or the school needs to perform a specific task in the public interest that is set out in law;

f) The processing of personal data is in the legitimate interests of the school, where we use your data in ways that people would reasonably expect and that have a minimal privacy impact. However, public authorities are more limited than private organisations in their ability to rely on this basis for processing personal data;

The lawful bases for processing special categories of data are:

(a) an individual has given explicit consent to the processing of personal data for one or more specified purposes, except where limited by law;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the school or a person under employment, social security and social protection law or a collective agreement under law;

(c) processing is necessary to protect the vital interests of a person or where the person is physically or legally incapable of giving consent;

(d) processing by non-for-profit bodies for legitimate activities with appropriate safeguards;

(e) processing relates to personal data which have been made public by a person;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest under law;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality;

(i) 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 quality and safety of health care and of medicinal products or medical devices, subject to the duty of confidentiality;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

The school must always demonstrate it processes information with safeguards in place to protect the fundamental rights and interests of the individual.

8. Consent

Where the school relies on consent or explicit consent as the lawful basis for processing, we will do this to by offering individuals real choice and control.

We will avoid making consent to processing a precondition of a service.

We will be clear and concise.

We keep our requests for consent separate from other terms and conditions.

We will be specific and ‘granular’ so that we get separate consent for separate things.

We will name any third parties (i.e. other groups or organisations) who will rely on the consent.

We will make it easy for people to withdraw consent and tell them how.

We will keep evidence of consent (who, when, how, and what we told people).

We will keep consent under review, and update it if anything changes.

For explicit consent we will ensure the individual provides a very clear and specific statement of consent.

9. Duty of confidentiality

Our staff and contractors abide by a common law duty of confidentiality. This means that personal information that has been given to a member of staff or a contractor by an individual should not be used or disclosed further, except as originally understood by that individual, or with their permission.

Our staff and contractors are subject to a Code a Conduct relating to confidentiality. Staff have a confidentiality clause in their contracts.

10. Information about criminal offences

The processing of information about criminal allegations, convictions or offences by the school is in accordance with our legal obligations.

We have a separate policy for the processing of this data.

11. Surveillance

The school operates CCTV for public safety and crime prevention. We operate under a Code of Practice prescribed by the Information Commissioner’s Office (ICO).

12. Children

The school pays particular protection to the collecting and processing of children’s personal data because they may be less aware of the risks involved.

Where we offer an online service, which is not a preventive or counselling service, directly to a child, only children aged 13 or over are able provide their own consent. For children under this age we obtain consent from whoever holds parental responsibility for the child.

13. Automated processing

Where the school relies on automated decision-making (making a decision solely by automated means without any human involvement) which affects an individual, we inform the individual; introduce simple ways for them to request human intervention or challenge a decision; and carry out regular checks to make sure that our systems are working as intended.

14. How we handle personal information - Privacy notices

The school provides privacy notices, which are statements to individuals about the collection and use of their personal data. The information includes our purposes for processing their personal data, retention periods for that personal data, and who it will be shared with.

This information is on the school's website, and individuals will be referred to it at the time we collect their personal data from them.

Where we obtain personal data from other sources, we provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

15. Individual Rights

Individuals whose data is processed by the school have a number of rights in law.

(a) The school will respond to a request by an individual for access to the information we hold about them. We will respond within one month. We may take longer than one month and up to three months if the request is complicated, and we will inform you of this. There is no charge for this service. We will provide the information in secure electronic format unless you prefer otherwise.

(b) The school will respond within one month to a request from an individual to have inaccurate personal data rectified (corrected), or completed if it is incomplete. Where the school can lawfully refuse to rectify the data, we will explain why.

(c) The school will respond within one month to a request from an individual to have personal data erased. Where the school can lawfully refuse to erase the data, we will explain why.

(d) The school will respond within one month to a request from an individual to move, copy or transfer personal data easily from the school's computer network to another in a safe and secure way. We will do this in a structured, commonly used and machine readable form and free of charge.

(e) The school will consider a request from an individual objecting to the processing of their personal data in relation to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

- direct marketing (including profiling); and

- processing for purposes of scientific/historical research and statistics.

We shall ensure that individuals know about their right to object when we first tell them about the processing and in our privacy notice.

16. Information sharing

The school believes that the duty to share information can be as important as the duty to protect information.

The school must have a compelling reason to share personal data. Sharing children's data with third parties can expose them to unintended risks if not done properly.

Before the school shares any data, we will:

- consider all the legal implications
- check if permission is needed to share the data
- confirm who needs the data, what data is needed and what they'll use it for
- make sure that the school has the ability to share the specified data securely
- check that the actions cannot be completed or verified without the data

16.1 Safeguarding

To keep children and young people safe in school, the school will need to share information appropriately, so the correct decisions can be made to protect them.

To keep children safe and make sure they get the support they need, the school can share information with other schools and children's social care teams. It is not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child.

The school's safeguarding lead will decide if personal data needs to be shared and will make sure they record:

- who they're sharing that information with
- why they're sharing the data
- whether they have consent from the pupil, parent or carer

16.2 Sharing with other schools

When a pupil moves to another school, our school will transfer their records to the new school. This includes the pupil's common transfer file and educational record. The school will:

- make sure we transfer the data securely
- transfer the record within 15 days of getting confirmation the pupil is registered at another school

- be able to trace the record during the transfer

16.3 Sharing with the Local Authority and Government Departments

The school has a statutory requirement to share personal data about your pupils with Department for Education (DfE) through the school census. The school **does not** need to get consent from pupils, parents or carers to share this data with the DfE.

Occasionally, the school may need to share personal information about our pupils with the local authority. For example:

- if a pupil shows signs of physical or mental abuse, you may need to pass this information on to children's services

16.4 Photographs

Photos will be used in school for many different reasons. The school will seek consent for each different use of a photograph.

The school must get consent to:

- share photos on the school's social media channels
- include photos of pupils and staff in our prospectus or other marketing material
- use a photo of a pupil in school displays
- take a photo for a newspaper article

If the school uses a photo of a pupil, the school will not include their name unless it has specific consent to do so.

The school will only use a photo in line with the consent provided and will make it clear how long the photograph will be used.

Photos used in the school's identity management systems for performing the public task of the school, but once a child is no longer a pupil at the school, these will be deleted.

16.5 Exam Results

The UK GDPR does not stop schools from publishing exam results online or in the local press.

You do not need to get consent from pupils, parents or carers to publish exam results. However, you should tell pupils where and how their results will be published before they're published. This gives them an opportunity to ask you to remove their results from the list should they wish to.

17. Transfers to other countries

Most of our processing occurs in the UK. This means that there are common standards for the processing of personal data. However, when personal data is transferred to the European Economic Area and third countries, the school assures itself that the transfer of personal data is covered by an adequacy decision in the data protection arrangements of that country, an appropriate safeguard or an exception.

18. Privacy by design

The school is committed to a privacy by design or privacy by default approach to building new systems and updating procedures for processing personal data. We use the best technology and human processes we can in order to limit the risks to privacy.

19. Data Protection Impact Assessments

The school carries out Data Protection Impact Assessments (DPIAs) when we introduce new technology or changes to the processing of personal data. The assessment identifies the risk to privacy from the individual's perspective and what steps can be taken to reduce this wherever possible.

20. Contractors

Where the school has a contractual relationship with another organisation or individual, we will ensure we are clear about the contractor's role, responsibilities and accountability in relation to personal information.

21. Information Security

The School has an Information Security policy. The purpose of this policy is to take appropriate technical and organisational measures to protect personal data.

22. Breaches

The school tries hard to prevent information breaches, but when these occur, there is an incident reporting and investigation procedure. Where a breach is a serious risk to the rights and freedoms of anyone, it will be reported to the Information Commissioner within 72 hours.

23. Data Protection Officer

The school has appointed a Data Protection Officer as required by law. Their role will be to ensure the compliance of the school with data protection law.

The School's Data Protection Officer can be contacted at:

schooldataprotectionofficer@doncaster.gov.uk

Tel 01302 737978

24. How to complain

If you think we have breached data protection, you can complain and we will respond within one month.

If you are still unhappy, the Data Protection Officer will consider your appeal. Their response will take up to one month.

Finally, individuals can take their complaint to the Information Commissioner's Office for a decision.

25. Service and benefit

Data protection is a big challenge when digital technology can collect and transmit huge volumes of personal data. For our staff, Governors and contractors we are positive about the benefits, and serious about our responsibilities. We are transparent and accountable, and we believe that we can both serve, and protect, the information of our employees, pupils, parents/carers.

26. References

UK GDPR is the retained EU law version of the General Data Protection Regulation (EU) 2016/679

Data Protection Act 2018

Directive (EU) 2016/680 Law Enforcement Directive

Information Commissioner's Office: www.ico.org.uk

27. List of related policies and procedures

The Data Protection Policy should be read with our:

Safeguarding Special Category Data Policy
Law Enforcement (Data Protection) Policy
Information Security Policy
Rights of Individuals Policy
Data Protection Impact Assessment Procedure