

Falcons Primary School



FALCONS
PRIMARY SCHOOL



DATA PROTECTION POLICY

Approved by GB Date: November 2025

Review Date: November 2026

School Vision and Ethos Statement

We encourage all members of the Falcons Community to respect one another, to know that everyone has an important part to play in making the school as good as it can be, to take responsibility and be responsible, to strive for excellence and to try one's best in everything we do.

Our vision for Falcons Primary School is to be recognised as a school that values uniqueness, where children are provided with the skills to enable them to become:

- * successful learners
- * responsible citizens
- * creative thinkers and
- * reflective individuals.

SIKH ETHOS

The school draws on the teaching of the Sikh faith and is committed to providing not only an academic education, but one that will also encompass an underlying message of unity, equality and respect. High morals, discipline, love, compassion and selfless service towards all regardless of faith, gender or colour. Falcon School will embrace a universal, inclusive approach to spirituality.

AIMS

To achieve our vision, we aim for all pupils, staff, governors and parents to:

- Work in unity to make Falcons School a welcoming, stimulating and successful school. Encourage good manners, self-discipline and the desire to be enthusiastic learners who grow into forward thinking responsible citizens who respect, value and care for themselves and others.
- Provide an ethos with clear boundaries and expectations, enabling all children to succeed and to reach their full potential confidently, in a safe and supportive environment.
- Become excellent lifelong learners who are independent and prepared for the wider world and aim high to achieve aspirational goals.

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

DATA PROTECTION POLICY

1	Aims	4
2	Why Have This Policy	4
3	Definitions	4
4	What We Do And Who Does It	5
5	Personal Data We Collect	6
6	Data Protection Principles	8
7	Our Commitment	8
8	Lawful, Fair, and Transparent Data Processing.....	9
9	The Rights of Data Subjects	9
10	How We Store Data.....	10
11	Data Accuracy	12
13	Accountability and Record Keeping	12
14	CCTV policy.....	13
15	Data Retention.....	133
16	Subject Access Requests.....	13
17	Data Breach	155
18	Training	166
19	Contact Details and Useful Websites	166
20	COMPLAINTS & THE INFORMATION COMMISSIONER OFFICE (ICO).....	17
21.	Review.....	177
Appendix A - Data (Use and Access) Act 2025 - Complaint Process		18

AIMS

Falcons Primary School collects and uses personal information about staff, pupils, parents, governors and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

WHY HAVE THIS POLICY

This Policy sets the School's obligations regarding the collection, processing, transfer, storage, and disposal of personal information. The procedures and principles set out herein must be followed at all times by the School, its employees, governors, agents, contractors, or other parties working on behalf of the School.

Falcons Primary School is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation 2016/679 and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

DEFINITIONS

UK-GDPR

The United Kingdom General Data Protection Regulation (UK-GDPR) is the UK's data privacy law that governs the processing of personal data from individuals inside the UK. The UK-GDPR was drafted as a result of the UK leaving the EU, which resulted in the EU's GDPR not applying domestically to the UK any longer.

Personal Data

The UK-GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special Categories of Personal Data

The UK-GDPR defines "Special Categories" of Personal Data as any information relating revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. Trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is also classed as "Special Categories" of Personal Data.

Data Subject

A data subject is an individual who is the subject of personal data. For example, schools hold personal data about pupils, making each pupil a data subject under the terms of the UK-GDPR.

Data Protection Officer

Role required by the General Data Protection Regulation (UK-GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with UK-GDPR requirements.

Data Controller

The Data Controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor

A data processor is distinct from the data controller for whom they are processing the personal data. An employee of a data controller, or a department or unit within the School which is processing personal data. The processor maybe a third party with which the school has a UK-GDPR compliant contract.

Data Breach

A data breach is an incident that involves the unauthorized or illegal viewing, access, retrieval, accidental deletion or not proper use of data by an individual, an organisation, application or service.

WHAT WE DO AND WHO DOES IT

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

The schools Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the schools compliance with the UK-GDPR. The DPO would also work with the school by providing guidance and to develop related policies. They will report to the highest level and liaise with the IOC as and when required.

The governing body has overall responsibility for ensuring that the school complies with its obligations under the General Data Protection Regulation. On a daily basis responsibilities lie with the Data Controller. In the absence of the Data Controller the Lead Processor will take up the role. The Data Protection Officer and the Data Controller 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.

PERSONAL DATA WE COLLECT

Falcons Primary School will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) This includes personal data collected directly from data subjects and a person with parental responsibility, personal data obtained from the LA, previous school or the DfE. Falcons Primary School only collects, processes, and holds personal data for the specific purposes (or for other purposes expressly permitted by the UK-GDPR). Data subjects are kept informed at all times of the purpose or purposes for which the school uses their personal data.

Parents and Pupils

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 the 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
- Attendance Information
- Pastoral information provided by parents in relation to illness, welfare etc.
- Details of any medical conditions and contact information
- Safety information (first aid, incidents)

We will only retain the data we collect for as long as is necessary 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. 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. We also share information with health professionals for immunization, height and weight and other routines. We do use information such as names to create passwords and login details for approved ICT systems but never share contact details with such companies.

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
- Ensure that we have relevant information for medical emergencies, next of kin contact etc.

Staff personal data includes, but is not restricted 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
- Appraisal information
- Contact information for next of kin

We will only retain the data we collect for as long as is necessary 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 can contact the school office of the Data Protection Officer, the Subject Access Request (SAR) procedure must be followed.

DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the UK-GDPR. The UK-GDPR sets out the following principles with which any party handling personal data must comply. The controller shall be responsible for and be able to demonstrate, compliance with the principles.

All personal data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- 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.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 UK-GDPR in order to safeguard the rights and freedoms of the data subject.
- 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.

OUR COMMITMENT

The school is committed to maintaining the data protection principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely

- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

At Falcons Primary School we ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The UK GDPR as amended by the Data (Use and Access) Act (DUAA) 2025 has seven conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions. :

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
- The processing is necessary to safeguard vulnerable individuals, crime prevention, and respond to emergencies.

THE RIGHTS OF DATA SUBJECTS

At Falcons Primary School Data Controller is the responsible for allowing data subjects to exercise their rights and to ensure that they can make effective use of them. The UK-GDPR sets out the following rights applicable to data subjects:

The right to be informed

In order to ensure that personal data are processed fairly, data controllers must provide certain minimum information to data subjects, regarding the collection and further processing of their personal data. The UK-GDPR adds that such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The right of access

Data subjects have the right to file a subject access request (SAR) and obtain from the data controller a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, and the categories of third parties to whom the data may be disclosed.

The right to rectification

Data subjects have the right to require the data controller to correct errors in personal data processed by (or on behalf of) that controller.

The right to erasure

Allows data subjects to require data controllers to delete their personal data where those data are no longer needed for their original purpose, or where the processing is based on the consent and the data subject withdraws that consent (and no other lawful basis for the processing exists).

The right to restrict processing

To restrict processing is a new right created under the UK-GDPR. In certain circumstances in which the relevant personal data either cannot be deleted (eg because the data are required for the purposes of exercising or defending legal claims) or where the data subject does not wish to have the data deleted, the data controller may continue to store the data, but the purposes for which the data can be processed are strictly limited.

The right to data portability

This permits the data subject to receive from the data controller a copy of his or her personal data in a commonly used machine-readable format, and to transfer their personal data from one data controller to another or have the data transmitted directly between data controllers.

The right to object

Data subjects continue to have a right to object to processing of their personal data on certain grounds

The rights with respect to automated decision-making and profiling

The rights related to automated decision making and profiling. The UK-GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

HOW WE STORE DATA

Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal information are kept secure when not in use. We carry out visual audits and regularly improve our practices.

- All records are stored in a central location. This is locked and only certain staff have access to these.

- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to notice boards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must ensure this is secure. Confidential data can only be taken out with the approval of the senior management team.
- Passwords that are secure are used to access school computers, laptops and other electronic devices.
- All electronic data information systems are password protected.
- Staff and pupils are reminded to change their passwords at regular intervals
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the School where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the UK-GDPR (which may include demonstrating to the School that all suitable technical and organisational measures have been taken).
- Encryption software is used to protect all portable devices and removable media, such as 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.

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. At Falcons Primary School we have adopted this approach when we

- are installing or adopting new ICT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- working with a new supplier that involves sharing
- using data for new purposes.

DATA ACCURACY

Data held will be as accurate and up to date as is reasonably possible. Every opportunity will be given to the data subject to update the information the school holds. If a data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable.

A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures

of the affected information will contain both versions of the information.

WHO WE SHARE DATA WITH

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. 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.

We also share information with health professionals for immunization, height and weight and other routines. We do use information such as names to create passwords and login details for approved ICT systems but never share contact details with such companies. Other agencies and professional bodies may include but not limited to:

- Educators and Exam Boards – to meet our legal obligations.
- Ofsted - to meet our legal obligations
- Auditors for Schools
- Police forces, courts, tribunals- when we are legally bound to do so.

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 Schools Data Protection Officer.

ACCOUNTABILITY AND RECORD KEEPING

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the school's other data protection-related policies, and with the UK-GDPR and other applicable data protection legislation. The school shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information.

- The name and details of the School, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the School, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the school (please refer to the School's Data Retention Policy); and

Detailed descriptions of all technical and organisational measures taken by the school to ensure the security of personal data.

14 CCTV POLICY

Please also see the CCTV policy. We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:

- detection and prevention of crimes, in the school and on the premises
- pupil behaviour management, discipline and exclusions
- staff disciplinary and associated processes and appeals
- maintaining a safe environment for the whole school community

DATA RETENTION

The school shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

For full details of the Schools approach to data retention, including retention periods for specific personal data types held by the School, please refer to our Data Retention Policy.

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

SUBJECT ACCESS REQUESTS

A Subject Access Request (SAR) enables individuals to find out what personal data you hold on them, why you hold it and who you disclose it to. The UK-GDPR enforces strict parameters on the way these requests are dealt with. Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

Following the UK-GDPR's guidelines all requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request.

The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to. Where a SAR has been made electronically, the information will be provided in a commonly used

electronic format. If the request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

In accordance with the Data (Use and Access) Act 2025, we are required to conduct searches that are reasonable and proportionate when responding to a SAR. If a request results in a substantial volume of data deemed to be unreasonable and disproportionate, we will notify you and offer an opportunity to refine the scope of your request. This allows you to specify the information you are seeking, enabling us to carry out a targeted search and provide the most relevant data.

SAR Procedure

- Data Subject or their Representative makes a request in writing to the school or the DPO
- School/DPO reply and request data subject to complete Subject Access Request Form
- School to verify the identity of the person making the request the following are accepted as evidence of identity:

Passport
Driving licence
Utility bills with current address
Birth / Marriage certificate
P45/P60
Credit Card or Mortgage statement

- The request is logged on the School DPO Portal If the initial request does not clearly identify the information required, then further enquiries will be made. The response time for subject access requests, once officially received, is 30 days. However the 30 days will not commence until after receipt of clarification of information sought.
- The school provides the information in line with the request
It must be noted any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings. If there are concerns over the disclosure of information, then additional advice should be sought. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained.

If information contained within the disclosure is difficult to read or illegible, then it should be retyped. Information can be provided at the school with a member of staff on hand to help and

explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Children have the same rights to access the information as adults as personal data about a child belongs to that child and not the person who has parental responsibility over that child. However, children below the age of 12 are generally not regarded to be mature or have enough understanding about their rights and the implications of a SAR. For an adult to make a SAR with respect to their child, the child must give consent or have a clear lack of understanding about their rights and the implications of a SAR. With this in mind most subject access requests from adults with parental responsibility of pupils at Falcons Primary School may be granted.

If you wish to complain about the process, please refer to Complaints Policy and later information in this policy.

DATA BREACH

In the case of a data breach, the person causing or noticing the breach should log the breach on the school portal. The portal will inform the Data Protection Officer and the Data Controller

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Unauthorised use or Access;
- Equipment Failure;
- Poor data destruction procedures;
- Human mistake;
- Cyber-attack;
- Hacking.
- Unforeseen circumstance such as fire or flood;
- Data not fully used or acted up on.

In most cases, the next stage would be for the DPO and/or Head teacher to fully investigate the breach. The DPO and/or Head teacher should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

The type of data;

- Is it sensitive;

- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency. On reviewing the breach, The Data Protection Officer or the Data Controller should not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with UK-GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

TRAINING

Our staff and governors are provided with UK-GDPR training as part of their induction process. UK-GDPR training will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary. As a school we ensure the senior management team fully understand UK-GDPR and its potential impact. All other staff are trained according to their roles and responsibilities. We stress how the UK-GDPR is the responsibility of the whole school community.

CONTACT DETAILS AND USEFUL WEBSITES

Data Protection Officer

PHP Law

Named DPO: John Walker

info@phplaw.co.uk

0300 3034360

6 Delamore Park | Cornwood | Ivybridge | PL21 9QP

Data Controller

Mrs. J Mann

Falcons Primary School

George Hine House

Gipsy Lane

Leicester

LE5 0TA

01164510050

COMPLAINTS & THE INFORMATION COMMISSIONER OFFICE (ICO)

In accordance with requirements set out by DUAA 2025, Falcons Primary has established a dedicated complaint procedure for data protection matters. Please see our Complaint Policy on school's website.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through a formal procedure. Please complete our dedicated form, and we will contact you with more details about the timescale and process.

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

Website: www.ico.org.uk

REVIEW

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Data Protection Officer, Head teacher or nominated representative.

APPENDIX A - DATA (USE AND ACCESS) ACT 2025 - COMPLAINT PROCESS

Introduction

Falcons Primary School is committed to protecting the privacy and personal data of its students, staff, parents/carers, governors and the wider school community. This policy outlines the procedure for handling complaints related to data usage and access, in accordance with the Data Usage Access Act (DUAA) and other relevant UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The UK GDPR documents as set out on our website provide an overview of how personal data is managed across our school.

This is an appendix to the main complaint policy and reflects the requirement for standalone data usage complaints to be handled using a separate procedure. Any complaint that is linked to other matters whether raised as a formal or informal complaint are to be dealt with under the standard complaint process as outlined within the main complaint policy.

Roles and responsibilities

The Data Controller (DC) is responsible for ensuring compliance with this policy and the legal obligations imposed by the UK GDPR, Data Protection Act 2018, Data Usage and Access Act 2025 and other relevant legislation. The DC will delegate day to day management of this to the relevant staff member and the DC will expect that staff member to investigate any complaint unless there is a conflict of interest, in which case the DC will appoint a suitable person.

The headteacher and leadership team are responsible for ensuring all staff are aware of this policy and their data protection obligations.

All staff members are responsible for handling personal data in a secure and lawful manner and for co-operating fully with any investigation into a data usage or access complaint.

Scope

This policy applies to all individuals who have dealings with Falcons Primary School and believe that their personal data has been used or accessed inappropriately, or that their rights under the DUAA and other data protection laws have been infringed.

This includes but is not limited to:

- current and former students
- parents/carers
- school staff (teaching, support, and administrative)
- governors
- volunteers

- contractors and suppliers

Principles

Fairness and transparency: All complaints will be handled in a fair, impartial, and transparent manner.

Confidentiality: Complaints and all related information will be treated with the utmost confidentiality, unless disclosure is required by law.

Timeliness: Complaints will be acknowledged and investigated in a prompt manner.

Compliance: All actions taken will comply with the DUAA, UK GDPR, DPA 2018, and other relevant legislation.

The complaint procedure

Step 1: Informal resolution

We encourage individuals to first attempt an informal resolution of their concerns. If you have a concern about data usage or access, you should, in the first instance, raise it with the relevant member of staff or senior person. Email your concerns to office@falconprimary.org for the attention of the Senior Leadership Team.

In many cases, issues can be resolved quickly and informally at this stage.

Step 2: Formal complaint submission

If the informal approach is not successful or deemed inappropriate, a formal complaint should be submitted in writing for the attention of the Headteacher.

The written complaint should include the following information:

1. your full name and contact details.
2. a clear and concise description of the complaint, including what happened, when it happened, and who was involved.
3. a description of the data involved and how you believe it was used or accessed inappropriately.
4. any relevant dates, times, or evidence.
5. details of any informal steps you have already taken to resolve the issue.
6. the desired outcome of the complaint.

Step 3: Acknowledgment and investigation

You will receive an acknowledgment of the written complaint within 5 working days of the setting receiving it.

The DC will conduct a thorough and impartial investigation into the complaint.

This may involve:

- interviewing the complainant
- interviewing relevant staff members
- reviewing school records, logs, and policies
- consulting with external legal or data protection experts if necessary

The Falcons Primary School will aim to complete the investigation and provide a substantive response within 20 working days of the complaint's acknowledgment. If the investigation is complex and requires more time, the DC will write to the complainant to explain the reason for the delay and provide a new estimated completion date.

Response

The DC will provide a formal written response to the complainant.

This response will include:

- the findings of the investigation.
- a clear and reasoned conclusion as to whether the DUAA or other data protection laws have been breached.
- details of any corrective action taken or planned to prevent a recurrence of the issue.
- the outcome of the complaint, including whether it has been upheld, partially upheld, or not upheld.
- information on the next steps available to the complainant if they remain dissatisfied.

Escalation

If the complainant is not satisfied with the school's final response, they have the right to escalate their complaint to the Information Commissioner's Office (ICO).

The ICO's contact details are as follows:

Website: <https://ico.org.uk>

Telephone: 0303 123 1113

Postal Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF