Part of the Branches Education Group

# DATA PROTECTION POLICY

| | | | |
|---|---|---|---|
| Approved By | Rebecca Warhurst | Head Teacher | Aug 2026 |
| Amendments Made | | | |
| Linked Policies | Safeguarding Policy | | |
| Signed | R Warhurst | Head Teacher | Aug 2026 |
| | L De Hayes | Governance Chair | Aug 2026 |
| Date Next Review | Aug 2027 | | |

# Contents

Statement of Intent ..... 3
1. Legal framework ..... 3
2. Applicable data ..... 4
3. Accountability ..... 5
4. Data protection officer (DPO) ..... 6
5. Lawful processing ..... 7
6. Consent ..... 9
7. The right to be informed ..... 10
8. The right of access ..... 11
9. The right to rectification ..... 12
10. The right to erasure ..... 12
11. The right to restrict processing ..... 13
12. The right to data portability ..... 14
13. The right to object ..... 15
14. Automated decision making and profiling ..... 16
15. Data protection by design and default ..... 17
16. Data Protection Impact Assessments (DPIAs) ..... 17
17. Data breaches ..... 18
18. Data security ..... 19
19. Safeguarding ..... 20
20. Publication of information ..... 21
21. Photography ..... 21
22. Cloud computing ..... 22
23. Data retention ..... 23
24. DBS data ..... 23
25. Monitoring and review ..... 23

## Statement of Intent

Silver Birch School is committed to protecting the rights and freedoms of individuals with regard to the processing of personal data. The school is required to collect, use and store certain information relating to employees, pupils, parents/carers, governors, volunteers, contractors and other stakeholders in order to carry out its statutory functions and provide education and support services.

The school recognises its responsibilities under UK data protection legislation and is committed to processing personal data lawfully, fairly and transparently. Appropriate technical and organisational measures are in place to ensure that personal information is protected against unauthorised access, accidental loss, destruction or damage.

From time to time, the school may be required to share personal information with external organisations, including the Local Authority (LA), the Department for Education (DfE), other educational settings, health professionals, safeguarding partners and children's services, where there is a lawful basis to do so.

The school recognises that effective safeguarding depends upon appropriate information sharing. Data protection legislation does not prevent the sharing of information where it is necessary to safeguard and promote the welfare of children. The school will ensure that all information sharing is undertaken in accordance with legal requirements and statutory guidance, including Keeping Children Safe in Education (KCSIE) 2026.

This policy ensures that all staff, governors and volunteers understand their responsibilities regarding data protection and sets out how the school complies with the principles of the UK General Data Protection Regulation (UK GDPR).

The school is committed to maintaining clear policies and procedures which support good information governance and promote a culture of accountability, transparency and security.

## 1. Legal Framework

This policy has due regard to all relevant legislation and statutory guidance, including, but not limited to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Education (Pupil Information) (England) Regulations 2005 (as amended)
- Privacy and Electronic Communications Regulations (PECR) 2003, where applicable

**This policy also has regard to the following guidance:**

- Information Commissioner's Office (ICO) Guide to the UK GDPR
- ICO Accountability Framework

- ICO Data Sharing Code of Practice
- ICO Guidance on Information Security and Data Breaches
- Department for Education (DfE) Data Protection Toolkit for Schools
- DfE Cyber Security Standards for Schools and Colleges
- Keeping Children Safe in Education (KCSIE) 2026 (effective from 1 September 2026)

**This policy operates in conjunction with the following school policies and procedures:**

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Information Security Policy
- Acceptable Use Policy
- Records Management and Retention Policy
- Freedom of Information Policy
- Staff Code of Conduct
- Data Breach Response Procedure
- CCTV Policy (where applicable)
- Confidentiality Policy

## 2. Applicable data

For the purpose of this policy, 'personal data' refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

'Sensitive personal data' is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

• Genetic data.

• Biometric data.

• Data concerning health.

• Data concerning a person's sex life.

• Data concerning a person's sexual orientation.

• Personal data which reveals:

- Racial or ethnic origin.

- Political opinions.

- Religious or philosophical beliefs.

- Trade union membership.

- Principles.

'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

• Under the control of official authority; or

• Authorised by domestic law.

The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

• The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

In accordance with the requirements outlined in the UK GDPR, personal data will be:

• Processed lawfully, fairly and in a transparent manner in relation to individuals.

• 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 incompatible with the initial purposes.

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

• Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are 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 are 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 individuals.

• 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.

The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

## 3. Accountability

Silver Birch School is committed to demonstrating compliance with the principles of the UK GDPR and Data Protection Act 2018 through appropriate technical and organisational measures. The school will maintain clear, comprehensive and transparent data protection practices and privacy information for all individuals whose personal data is processed.

The school will maintain records of processing activities where required by law and as part of its accountability obligations. Records will be reviewed regularly to ensure they remain accurate and up to date.

Records of processing activities will include:

- The name and contact details of the school and, where applicable, its Data Protection Officer (DPO).
- The purposes of processing personal data.
- Categories of data subjects and personal data processed.
- The lawful basis for processing.
- Categories of recipients to whom personal data may be disclosed.
- Retention periods for different categories of personal data.
- Details of any transfers of personal data outside the UK, including safeguards applied.
- A description of the technical and organisational security measures in place to protect personal data.

The school will maintain documentation and evidence of compliance where appropriate, including:

- Privacy notices.
- Records of consent, where consent is relied upon as the lawful basis for processing.
- Contracts and agreements with data processors.
- Data Protection Impact Assessments (DPIAs).
- Records of personal data breaches and actions taken.
- Information asset registers.
- Data sharing agreements.
- Staff training records relating to data protection, information security and cyber security.

The school will apply the principles of **Data Protection by Design and by Default** when developing new systems, procedures and processes involving personal data. This includes:

- Collecting and processing only the personal data necessary for the specified purpose.
- Ensuring personal data is accurate and kept up to date.
- Restricting access to personal data on a need-to-know basis.

- Applying appropriate security controls, including encryption, password protection and multi-factor authentication where appropriate.
- Pseudonymising or anonymising personal data where possible.
- Ensuring transparency regarding how personal data is used.
- Regularly reviewing and strengthening information security measures.

Data Protection Impact Assessments (DPIAs) will be undertaken where processing is likely to result in a high risk to the rights and freedoms of individuals, or where required by law or ICO guidance.

## 4. Data Protection Officer (DPO)

In accordance with UK data protection legislation, the school has appointed a Data Protection Officer (DPO) who acts as the central point of contact for data protection matters.

The DPO will:

- Inform and advise the school, governors and staff of their obligations under data protection legislation.
- Monitor the school's compliance with UK GDPR, the Data Protection Act 2018 and associated policies and procedures.
- Provide advice and guidance on Data Protection Impact Assessments (DPIAs).
- Support the investigation and management of personal data breaches.
- Promote awareness of data protection responsibilities through training and guidance.
- Liaise with the Information Commissioner's Office (ICO).
- Act as the first point of contact for individuals regarding the processing of their personal data.

The DPO is responsible for:

- Promoting a culture of good information governance across the school.
- Supporting compliance with data protection, information security and cyber security requirements.
- Monitoring data protection risks and advising on measures to reduce them.
- Reviewing data protection practices and procedures.
- Providing independent advice on the use, sharing, retention and disposal of personal data.
- Keeping senior leaders and governors informed of significant data protection risks and compliance matters.

The school will ensure that the DPO:

- Has expert knowledge of data protection law and practice appropriate to the education sector.

- Is able to perform their role independently and without conflict of interest.
- Is involved in data protection matters in a timely manner.
- Has access to appropriate resources, training and support to perform their duties effectively.
- Has direct access to the Headteacher and Governing Board.

The DPO will report periodically to the Governing Board on the school's compliance with data protection legislation, significant risks, data breaches and areas for improvement.

**5. Lawful Processing**

Silver Birch School will identify and document the appropriate lawful basis for processing personal data before any processing takes place.

Under UK GDPR, the school will process personal data only where one or more of the following lawful bases applies:

- The individual has given consent for the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract with the individual or to take steps at their request prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the school is subject.
- Processing is necessary to protect the vital interests of the individual or another person.
- 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 school.
- Processing is necessary for the purposes of legitimate interests pursued by the school or a third party, except where those interests are overridden by the interests, rights or freedoms of the individual. Legitimate interests will generally not apply where the school is carrying out its public functions.

The school will ensure that personal data is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

**Special Category Data**

The school recognises that certain types of personal data require additional protection. Special category data will only be processed where a lawful basis for processing under Article 6 UK GDPR exists and an additional condition under Article 9 UK GDPR is satisfied.

The school may process special category data where:

- The individual has given explicit consent.
- Processing is necessary for carrying out obligations and exercising specific rights in the field of employment, social security or social protection law.
- Processing is necessary to protect the vital interests of an individual where they are incapable of giving consent.

- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the provision of health, social care or treatment.
- Processing is necessary for public health purposes.
- Processing is necessary for archiving, research or statistical purposes in accordance with applicable legislation.

The school will ensure that appropriate safeguards are in place whenever special category data is processed.

**Transparency and Privacy Information**

The school is committed to processing personal data fairly and transparently. Individuals will be informed about:

- The identity and contact details of the school.
- The purpose for which their personal data is being processed.
- The lawful basis for processing.
- The categories of personal data being processed.
- Any recipients or categories of recipients who may receive the data.
- How long the data will be retained.
- Their rights under UK data protection legislation.
- Their right to lodge a complaint with the Information Commissioner's Office (ICO).

The school provides privacy notices to the following groups:

- Pupils and parents/carers.
- Employees and prospective employees.
- Governors and trustees.
- Volunteers.
- Contractors and suppliers.
- Visitors and other third parties where appropriate.

**Safeguarding and Vital Interests**

The school recognises that there may be circumstances where personal information needs to be shared to protect a child or vulnerable individual from harm.

Where there are safeguarding concerns, the school will share information with relevant agencies where it is lawful, necessary and proportionate to do so. The UK GDPR and Data Protection Act 2018 do not prevent the sharing of information for safeguarding purposes where failure to share could place a child at risk of harm. Appropriate records of decisions and actions taken will be maintained.

**Children's Data**

Where the school processes children's personal data, it will take account of the age, maturity and understanding of the child, ensuring that processing is fair and transparent.

Where consent is relied upon as the lawful basis for processing, the school will ensure that consent is obtained from the appropriate individual and that any safeguarding considerations are fully taken into account.

## 6. Consent

Where consent is relied upon as the lawful basis for processing personal data, Silver Birch School will ensure that consent is:

- Freely given.
- Specific.
- Informed.
- Unambiguous.
- Given through a clear affirmative action.

Consent will not be inferred from silence, inactivity or pre-ticked boxes.

Individuals have the right to withdraw consent at any time. The withdrawal of consent will be acted upon promptly and will not affect the lawfulness of processing undertaken before consent was withdrawn.

The school will maintain records of:

- When consent was obtained.
- How consent was obtained.
- What information was provided to the individual at the time consent was obtained.
- Any withdrawal of consent.

The school recognises that consent is not always the most appropriate lawful basis for processing personal data. Where another lawful basis is more appropriate, the school will rely on that basis rather than consent.

Consent may be sought for activities including, but not limited to:

- The use of pupil photographs and videos.
- Promotional and marketing materials.
- Educational visits and activities where specific consent is required.
- The use of online services where consent is the appropriate lawful basis.

When obtaining consent relating to children, the school will take account of the child's age and understanding, parental responsibility arrangements and relevant safeguarding considerations.

Consent forms and procedures will be reviewed regularly to ensure they remain compliant with UK GDPR requirements and reflect current school practices.

## 7. The Right to Be Informed

Silver Birch School is committed to ensuring that individuals understand how and why their personal data is collected, used and shared.

The school will provide privacy notices to pupils, parents/carers, employees, governors, volunteers, contractors and other relevant individuals. Privacy notices will be written in clear, concise and accessible language. Where information is provided to children, it will be presented in an age-appropriate format that can be easily understood.

Where the school collects personal data directly from an individual, privacy information will be provided at the time the data is collected. Where personal data is obtained from another source, privacy information will be provided within one month of obtaining the data, or sooner where required by law.

Privacy notices will include:

- The identity and contact details of the school.
- The contact details of the Data Protection Officer (DPO).
- The purposes for which personal data is processed.
- The lawful basis for processing.
- Where applicable, the legitimate interests relied upon by the school or a third party.
- The categories of personal data collected and processed.
- Any recipients or categories of recipients who may receive the information.
- Details of any transfers of personal data outside the UK and the safeguards in place.
- How long personal data will be retained, or the criteria used to determine retention periods.
- The rights available to individuals under data protection legislation.
- The right to withdraw consent where consent is the lawful basis for processing.
- The right to lodge a complaint with the Information Commissioner's Office (ICO).
- Details of any automated decision-making or profiling where applicable.

Where the provision of personal data is required by law, contract, or as part of the school's statutory functions, individuals will be informed of this and of any potential consequences of failing to provide the information.

The school will regularly review privacy notices to ensure they remain accurate, transparent and compliant with current legislation and guidance.

## 8. The Right of Access

Under UK data protection legislation, individuals have the right to obtain confirmation that their personal data is being processed and to request access to that data by making a Subject Access Request (SAR).

The school will take reasonable steps to verify the identity of the individual making the request before providing any information.

Subject Access Requests will normally be responded to without undue delay and, in any event, within one calendar month of receipt of the request and verification of identity where required.

Information will usually be provided free of charge. However, the school may charge a reasonable fee or refuse to act on a request where it is manifestly unfounded or excessive, particularly where requests are repetitive. Any fee charged will reflect the administrative costs incurred.

Where a request is made electronically, and unless otherwise requested, information will be provided in a commonly used electronic format.

**Requests Made by or on Behalf of Children**

Children have the same rights of access to their personal data as adults. The school will consider each request on a case-by-case basis, taking into account the child's age, maturity and ability to understand their rights.

Where the school is satisfied that a child is competent to understand their rights, information will normally be provided directly to the child. Where a parent or individual with parental responsibility makes the request on behalf of a child, the school will consider whether the parent is entitled to act on the child's behalf and whether disclosure is in the child's best interests.

**Complex Requests**

Where a request is particularly complex or where multiple requests are received from the same individual, the school may extend the response period by up to two further months. The individual will be informed within one month of receipt of the request and provided with an explanation for the extension.

Where the school processes a large amount of information relating to an individual, it may ask the requester to clarify the scope of the request. Any request for clarification will be made promptly and the school will provide assistance where necessary to help the individual identify the information sought.

**Protecting the Rights of Others**

The school will ensure that information provided in response to a Subject Access Request does not adversely affect the rights and freedoms of other individuals.

Where necessary, the school may:

- Redact information relating to other individuals.
- Seek consent from third parties before disclosure.
- Withhold information where disclosure would be unlawful or where an exemption applies.

Where all or part of a request is refused, the school will explain the reasons for its decision and advise the individual of their right to complain to the Information Commissioner's Office (ICO) and to seek a judicial remedy.

### 9. The Right to Rectification

Individuals, including children, have the right to request that inaccurate or incomplete personal data is corrected without undue delay.

Silver Birch School will respond to requests for rectification within one calendar month of receipt. Where a request is particularly complex, the response period may be extended by up to two further months. The individual will be informed of any extension and the reasons for it within the initial one-month period.

The school will take reasonable steps to ensure that personal data is accurate, complete and kept up to date. Particular attention will be given to information that may significantly affect an individual or be used to make decisions about them.

Where the accuracy of personal data is disputed, the school may temporarily restrict the processing of that data while the matter is investigated.

Where personal data has been shared with third parties and is subsequently corrected, the school will, where practicable, inform those third parties of the rectification.

Requests for rectification will normally be dealt with free of charge. However, where a request is manifestly unfounded or excessive, particularly if repetitive, the school may:

- Charge a reasonable administrative fee; or
- Refuse to act on the request.

Where the school refuses a request for rectification, or determines that the information is accurate and does not require amendment, the individual will be informed of:

- The reasons for the decision.
- Their right to complain to the Information Commissioner's Office (ICO).
- Their right to seek a judicial remedy.

### 10. The Right to Erasure

Individuals, including children, have the right to request the deletion of their personal data in certain circumstances. This right is commonly referred to as the "right to be forgotten".

The school will consider all requests for erasure on a case-by-case basis and will respond without undue delay and normally within one calendar month.

An individual may request erasure where:

- The personal data is no longer necessary for the purpose for which it was collected or processed.

- Consent was the lawful basis for processing and that consent has been withdrawn.
- The individual has successfully objected to the processing of their personal data.
- The personal data has been processed unlawfully.
- The personal data must be erased to comply with a legal obligation.
- The personal data was collected in relation to the provision of online services to a child.

The right to erasure is not absolute. The school may refuse a request where processing is necessary:

- To comply with a legal obligation.
- To perform a task carried out in the public interest or in the exercise of official authority.
- For reasons of public health.
- For archiving, research or statistical purposes where deletion would seriously impair those purposes.
- For the establishment, exercise or defence of legal claims.
- For safeguarding purposes where information must be retained to protect a child or vulnerable individual.
- To comply with statutory education, safeguarding, employment, financial or health and safety record-keeping requirements.

As schools frequently process personal data as part of their public task and legal obligations, there will be circumstances where records cannot be erased even when requested. This applies particularly to safeguarding records, attendance records, special educational needs records, employment records and statutory educational records where retention is required by law or guidance.

Where a request is refused, the school will explain:

- The reasons for the decision.
- The individual's right to complain to the Information Commissioner's Office (ICO).
- Their right to seek a judicial remedy.

Requests for erasure will normally be processed free of charge. However, where requests are manifestly unfounded or excessive, particularly if repetitive, the school may charge a reasonable administrative fee or refuse to act on the request.

Where personal data has been shared with third parties and the school is required to erase that data, reasonable steps will be taken to inform those third parties unless doing so is impossible or would involve disproportionate effort.

Where personal data has been published online by the school and erasure is required, reasonable steps will be taken to inform other data controllers processing the information that the individual has requested the removal of links, copies or replications of that data.

When considering requests relating to children's data, the school will take account of the child's age, understanding and the circumstances in which the information was collected, while balancing any legal or safeguarding duties requiring retention of the data.

## 11. Right to Restrict Processing

Individuals have the right to request the restriction of the processing of their personal data in certain circumstances.

Silver Birch School will restrict the processing of personal data where:

- An individual contests the accuracy of personal data, pending verification of its accuracy.
- An individual has objected to processing and the school is considering whether its legitimate grounds override those of the individual.
- Processing is unlawful, and the individual requests restriction rather than erasure.
- The school no longer requires the personal data for processing purposes, but the individual requires it for the establishment, exercise or defence of legal claims.

Where processing has been restricted, the school will continue to store the personal data but will not otherwise process it unless:

- The individual has given consent.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is necessary for the protection of the rights of another person.
- The processing is necessary for reasons of substantial public interest.

The school will take reasonable steps to ensure that restricted data is clearly identified and inaccessible to staff or systems that do not require access. This may include temporarily removing data from active systems, limiting user access permissions or suspending publication of information where appropriate.

Where personal data subject to restriction has been shared with third parties, the school will inform those recipients of the restriction where required, unless this proves impossible or involves disproportionate effort.

The school will inform the individual before any restriction is lifted.

The school may refuse a request where an exemption applies or where the request is manifestly unfounded or excessive. In such cases, the individual will be informed in writing of:

- The reasons for the decision.
- Their right to request a review of the decision.
- Their right to complain to the Information Commissioner's Office (ICO).
- Their right to seek a judicial remedy.

The school will normally respond to requests without undue delay and within one month of receipt.

## 12. Right to Data Portability

Individuals have the right, in certain circumstances, to receive personal data they have provided to the school in a structured, commonly used and machine-readable format and to transmit that data to another organisation.

The right to data portability applies only where:

- The processing is based on the individual's consent or the performance of a contract.
- The processing is carried out by automated means.
- The request relates to personal data provided by the individual.

The right to data portability does not generally apply to personal data processed by schools under their statutory functions, legal obligations or public task responsibilities.

Where a valid request is received, the school will:

- Provide the personal data in a structured, commonly used and machine-readable format.
- Provide the information free of charge, unless the request is manifestly unfounded or excessive.
- Where technically feasible and requested by the individual, transmit the data directly to another organisation.

When responding to a data portability request, the school will consider the rights and freedoms of other individuals whose personal data may be included within the information requested.

The school is not required to adopt, maintain or implement systems that are technically compatible with those used by other organisations.

The school will normally respond to requests without undue delay and within one month of receipt. Where a request is complex or multiple requests have been received from the same individual, the response period may be extended by up to two additional months. In such cases, the individual will be informed within one month of receipt of the request and provided with an explanation for the delay.

Where the school decides not to take action in response to a request, it will inform the individual without undue delay and within one month of receipt of the request, explaining:

- The reasons for the decision.
- Their right to complain to the Information Commissioner's Office (ICO).
- Their right to seek a judicial remedy.

## 13. Right to Object

Individuals have the right to object to the processing of their personal data in certain circumstances.

Silver Birch School will inform individuals of their right to object through its privacy notices and other relevant communications. Information about this right will be presented in a clear and accessible manner.

Individuals may object to processing where it is based on:

- The performance of a task carried out in the public interest.
- Legitimate interests pursued by the school or a third party.
- Direct marketing purposes.
- Scientific or historical research purposes, or statistical purposes.

**Objections to Public Task or Legitimate Interest Processing**

Where an objection relates to processing carried out under a public task or legitimate interests basis, the individual must explain how their particular situation gives rise to the objection.

The school will carefully consider each objection and will stop processing the personal data unless:

- The school can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual; or
- The processing is necessary for the establishment, exercise or defence of legal claims; or
- The processing is required for the performance of a statutory duty or public task.

**Objections to Direct Marketing**

Where personal data is processed for direct marketing purposes, individuals have an absolute right to object.

Upon receiving an objection, the school will stop processing the personal data for direct marketing purposes without undue delay.

The school will retain only sufficient information to ensure that the individual's preference is respected in future communications.

**Objections to Research and Statistical Processing**

Individuals have the right to object to processing for research or statistical purposes where the objection relates to their particular circumstances.

However, the school may continue processing where it can demonstrate that the processing is necessary for the performance of a task carried out in the public interest.

**Handling Objections**

The school will maintain records of all objections received, including the actions taken and the outcome of the request.

Individuals may submit objections in writing, electronically, by telephone or in person. The school may seek clarification where necessary to ensure the request is properly understood.

The school will respond to objections without undue delay and normally within one month of receipt. Where a request is particularly complex or multiple requests are received from the same individual, the response period may be extended by up to two further months. The individual will be informed of any extension and the reasons for it.

Where the school decides not to take action in response to an objection, it will inform the individual of:

- The reasons for the decision.
- Their right to complain to the Information Commissioner's Office (ICO).
- Their right to seek a judicial remedy.

## 14. Automated Decision-Making and Profiling

Silver Birch School does not normally make decisions about individuals solely by automated means where those decisions have legal or similarly significant effects.

Where the school proposes to use automated decision-making or profiling activities, it will ensure compliance with UK GDPR requirements and implement appropriate safeguards to protect the rights and freedoms of individuals.

The school will only carry out solely automated decision-making where:

- It is necessary for entering into or performing a contract.
- It is authorised by law.
- The individual has provided their explicit consent.

The school will not normally use solely automated decision-making in relation to pupils. Any proposal to do so will be subject to careful consideration of legal, ethical and safeguarding implications.

Where automated decision-making or profiling is undertaken, the school will:

- Complete a Data Protection Impact Assessment (DPIA) before implementation.
- Assess and mitigate risks relating to accuracy, bias, discrimination and fairness.
- Ensure that processing is transparent and that affected individuals are informed about how decisions are made.
- Regularly review the effectiveness and fairness of automated processing systems.
- Maintain appropriate security measures to protect personal data.

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, where that decision produces legal effects or similarly significant effects.

Where such processing takes place, individuals will have the right to:

- Obtain human intervention.
- Express their views.
- Request an explanation of the decision.
- Challenge the outcome and request a review.

**Profiling**

Where profiling is carried out, the school will ensure that:

- Processing is lawful, fair and transparent.

- Individuals are provided with meaningful information about the logic involved and the potential consequences of the processing.
- Appropriate measures are in place to identify and correct inaccuracies.
- Suitable technical and organisational controls are implemented to prevent bias, discrimination or unfair outcomes.
- Personal data is processed securely and only for legitimate educational, safeguarding, employment or administrative purposes.

Silver Birch School will implement the principles of **Data Protection by Design and by Default** in accordance with UK GDPR requirements. Data protection considerations will be embedded into all new projects, systems, services, policies and procedures that involve the processing of personal data. The school will ensure that personal data is processed in a manner which is lawful, fair, transparent, secure and limited to what is necessary for the specified purpose.When developing or reviewing systems and processes, the school will consider:

- The nature, scope, context and purpose of the processing.
- The risks to the rights and freedoms of individuals.
- Appropriate technical and organisational measures to reduce those risks.
- Information security and cyber security requirements.
- Safeguarding requirements where children's personal data is involved.

The school will implement Data Protection by Design and by Default through measures including:

- Considering data protection requirements from the earliest stages of any project or procurement process.
- Collecting and processing only the personal data necessary to fulfil the intended purpose.
- Limiting access to personal data on a need-to-know basis.
- Applying appropriate security controls, including secure passwords, encryption and multi-factor authentication where appropriate.
- Configuring systems and applications to provide privacy-friendly default settings.
- Reviewing and minimising data retention periods where appropriate.
- Ensuring that suppliers and third-party providers meet the school's data protection and security requirements.
- Supporting staff through training and guidance on information governance and data protection.
- Promoting clear and transparent privacy information that can be easily understood by pupils, parents/carers, staff and other stakeholders.
- Ensuring the Data Protection Officer (DPO) is involved in projects where personal data protection issues may arise.

The school will regularly review its technical and organisational measures to ensure they remain effective and proportionate to emerging risks and technologies.

## 16. Data Protection Impact Assessments (DPIAs)

Silver Birch School will undertake Data Protection Impact Assessments (DPIAs) where processing is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA is a process designed to help identify, assess and minimise data protection risks before new processing activities commence. DPIAs also support compliance with UK GDPR accountability requirements and demonstrate that privacy risks have been considered appropriately.

The school will carry out a DPIA when introducing new technologies, systems or processes that involve personal data, including where processing is likely to be high risk.

Examples of processing that may require a DPIA include:

- Large-scale processing of special category data.
- Processing involving criminal offence data.
- Systematic monitoring of individuals.
- The introduction of new information management systems.
- CCTV or surveillance technologies.
- Biometric systems.
- Artificial intelligence (AI) or automated decision-making technologies.
- Significant data sharing arrangements involving sensitive personal information.
- Projects involving vulnerable individuals or children where privacy risks may be heightened.

A DPIA will include:

- A description of the proposed processing activity and its purpose.
- An assessment of the necessity, proportionality and lawful basis for the processing.
- Identification and assessment of potential risks to individuals.
- Consideration of the impact on children's rights and freedoms where appropriate.
- Details of measures that will be implemented to mitigate identified risks.

- Evidence of consultation with relevant stakeholders where appropriate, including the DPO.

The DPO will advise on whether a DPIA is required and will provide guidance throughout the process.

Where a DPIA identifies a high residual risk that cannot be adequately mitigated, the school will consult the Information Commissioner's Office (ICO) before commencing the processing activity.

DPIAs will be reviewed periodically and whenever there are significant changes to the nature, scope or purpose of the processing.

**17. Data Breaches**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Silver Birch School will maintain effective procedures for identifying, reporting, investigating and managing personal data breaches. All staff, governors, volunteers and contractors are expected to report any actual, suspected or potential data breach immediately in accordance with the school's Data Breach Response Procedure.

The Headteacher will ensure that all staff receive appropriate training and guidance so they understand:

- What constitutes a personal data breach.
- How to identify and report a breach.
- Their responsibilities for protecting personal information.
- The procedures for responding to a breach.

On becoming aware of a suspected breach, the school will take immediate steps to:

- Contain the breach and minimise any impact.
- Assess the nature and extent of the incident.
- Identify the individuals and data affected.
- Evaluate the risks to individuals' rights and freedoms.
- Determine whether notification is required.

The Data Protection Officer (DPO), in conjunction with senior leaders where appropriate, will coordinate the school's response and advise on the need for notification to the Information Commissioner's Office (ICO) and affected individuals.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will notify affected individuals without undue delay and provide information about:

- The nature of the breach.
- The likely consequences.
- Measures taken or proposed to address the breach.
- Steps individuals can take to protect themselves.

The school will maintain a record of all personal data breaches, regardless of whether they are reported to the ICO. Breach records will include:

- The facts relating to the breach.
- The effects of the breach.
- Actions taken to contain and remedy the breach.
- Decisions regarding notification.

Following any data breach, the school will review the circumstances surrounding the incident and implement measures to reduce the risk of recurrence. This may include improvements to procedures, technical controls, staff training or disciplinary action where appropriate.

Failure by staff to comply with data protection and information security requirements may result in disciplinary action in accordance with the school's disciplinary procedures.

## 18. Data Security

Silver Birch School is committed to maintaining the confidentiality, integrity and availability of personal data through appropriate technical and organisational security measures.

All staff are responsible for ensuring that personal data is handled securely and in accordance with this policy, the Information Security Policy and any related procedures.

**Physical Security**

Paper records containing personal or confidential information will:

- Be stored securely in locked cabinets, drawers or rooms when not in use.
- Only be accessible to authorised personnel.
- Not be left unattended in public or unsecured areas.
- Be transported securely where they need to be taken off-site.

Visitors will not have access to confidential or personal information and will be appropriately supervised whilst on school premises.

The security of school buildings, storage facilities and access arrangements will be reviewed regularly and additional security measures implemented where necessary.

**Digital Security**

The school will implement appropriate technical controls to protect personal data, including:

- Secure user accounts and passwords.

- Multi-factor authentication where appropriate.
- Encryption of personal and sensitive data.
- Appropriate firewall, malware protection and network security controls.
- Secure backup and recovery arrangements.
- Access controls based on business need.
- Regular software updates and security patch management.
- Monitoring and auditing of access to systems where appropriate.

The school will align its information security arrangements with relevant DfE cyber security standards and best practice guidance.

**Remote and Mobile Working**

Where staff access school systems remotely or work from home, they must use approved systems and follow the school's security requirements.

Personal devices should only be used for school business where authorised and where appropriate security controls have been applied.

Staff must take reasonable precautions to protect personal data when working remotely, including:

- Preventing unauthorised access to devices and documents.
- Locking devices when unattended.
- Storing information securely.
- Avoiding the use of unsecured public Wi-Fi networks where possible.

**Email and Information Sharing**

Staff must take care when sending emails containing personal information.

Before sharing personal data, staff must ensure that:

- There is a lawful basis for sharing the information.
- The information is being shared with the correct recipient.
- Appropriate security measures are in place.
- The sharing is consistent with privacy notices and data-sharing arrangements where applicable.

Where particularly sensitive or confidential information is being shared electronically, additional security measures such as encryption, password protection or secure transfer systems will be used where appropriate.

Group emails to parents and external recipients should normally use blind carbon copy (BCC) where recipients do not need to see each other's email addresses.

**Business Continuity and Recovery**

The school will maintain appropriate backup, continuity and disaster recovery arrangements to ensure that critical information and systems can be restored in the event of an incident.

The Headteacher supported by relevant ICT providers, is responsible for ensuring that appropriate business continuity arrangements are maintained and reviewed.

**Disposal of Information and Equipment**

Personal data will be disposed of securely in accordance with the school's Records Management and Retention Policy.

- Confidential paper records will be cross-cut shredded or disposed of through approved confidential waste services.
- Electronic records will be securely deleted when no longer required.
- ICT equipment and storage devices will be securely wiped or destroyed prior to disposal, in accordance with ICO guidance and recognised industry standards.

**Monitoring and Compliance**

The school will regularly test, review and evaluate the effectiveness of its data security measures.

Any deliberate or negligent failure to comply with data protection or information security requirements may result in disciplinary action and, where appropriate, referral to external authorities.

## 19. Safeguarding

Silver Birch School recognises that effective safeguarding depends upon the appropriate sharing of information and that data protection legislation does not prevent the sharing of information where this is necessary to safeguard and promote the welfare of children. Staff will ensure that concerns about a child's safety or wellbeing are shared promptly, lawfully and proportionately with relevant agencies and professionals where necessary.

The school will ensure that information required to identify, assess and respond to safeguarding concerns is shared appropriately and without unnecessary delay.

Where decisions are made regarding the sharing of safeguarding information, the Designated Safeguarding Lead (DSL), or an appropriate member of staff acting on their behalf, will ensure that a record is maintained of:

- Whether information was shared.
- What information was shared.
- Who the information was shared with.
- The purpose of the information sharing.
- The lawful basis for sharing the information.
- Whether consent was sought.

- Where consent was not sought, the reasons for this decision.
- Any advice received from safeguarding partners, the Local Authority, police, social care or other relevant agencies.

The school will seek consent to share personal information where appropriate and where it is safe and lawful to do so. However, consent will not be sought where this may place a child at increased risk of harm, prejudice the prevention or detection of crime, or delay action required to safeguard a child.

All safeguarding information will be handled in accordance with the school's Safeguarding and Child Protection Policy, Records Management and Retention Policy, and applicable data protection legislation.

Staff will receive appropriate training regarding confidentiality, information sharing and safeguarding responsibilities to ensure that decisions are made in the best interests of children.

**20. Publication of Information**

Silver Birch School is committed to openness and transparency and will make information available in accordance with the Freedom of Information Act 2000 and its Freedom of Information Publication Scheme.

The Publication Scheme, available on the school's website, identifies information that is routinely made available to the public, including:

- School policies and procedures.
- Governance information, including approved minutes where appropriate.
- Annual reports and statutory information.
- Financial information required to be published by law.
- Curriculum and educational information.
- Information relating to the school's operation and performance.

The school will ensure that information covered by the Publication Scheme is made available promptly and in an accessible format wherever possible.

The school will not publish personal information on its website or through other public communication channels unless there is a lawful basis to do so. Where consent is required, appropriate consent will be obtained and recorded before publication.

Particular care will be taken when publishing information relating to children. The school will consider safeguarding, privacy and data protection implications before publishing photographs, videos or other identifying information.

Prior to publication, staff will ensure that documents and images are checked to remove personal data, hidden information, version histories and metadata which could result in the inadvertent disclosure of confidential information.

The school will regularly monitor and review information published on its website and other digital platforms to ensure that it remains accurate, relevant, lawful and compliant with data protection requirements.

## 21. Photography

Silver Birch School recognises that images of identifiable individuals constitute personal data and will be processed in accordance with UK data protection legislation.

**Photography and Video Recording**

The school recognises the educational and promotional value of photographs and videos and will ensure that their use is lawful, fair and transparent.

Parents and carers will be informed about how photographs and video recordings may be used by the school. Where consent is required, appropriate consent will be obtained and recorded before images are used.

Photographs and videos of pupils may be used for educational purposes, displays, school publications, newsletters, promotional materials and the school website where there is an appropriate lawful basis for doing so.

The school will take appropriate steps to protect pupils when publishing images or recordings, including consideration of safeguarding, privacy and individual circumstances.

All use of photography and video will be undertaken in accordance with the school's Photography and Video Policy and Safeguarding and Child Protection Policy.

**Parents, Visitors and School Events**

Parents, carers and visitors may take photographs or videos during school performances and events for personal and domestic use only.

Photographs and recordings taken at school events must not be used for commercial purposes or in a manner that may compromise the privacy, dignity or safety of any child or member of staff.

The school requests that parents and visitors do not publish photographs or videos containing children other than their own on social media or other publicly accessible platforms without the appropriate consent of those concerned.

## 22. Cloud Computing

The school uses cloud-based systems and services where these support educational, safeguarding, administrative and operational needs.

All cloud services used by the school will be subject to appropriate due diligence to ensure compliance with UK GDPR, data protection legislation and the Department for Education's cyber security expectations.

The school will ensure that:

- Access to cloud-based systems is restricted to authorised users.
- Individual user accounts are provided where appropriate.
- Strong password controls and multi-factor authentication are used where available.
- User accounts are reviewed regularly and removed promptly when no longer required.
- Personal data is protected during transmission and storage through appropriate security measures.
- Access permissions are based on roles and business need.
- Audit logs and monitoring tools are utilised where available to identify unauthorised access or activity.

Before using a cloud service, the school will:

- Undertake an assessment of privacy, security and compliance risks.
- Ensure that an appropriate contract and Data Processing Agreement (DPA) are in place.
- Confirm the provider's responsibilities relating to confidentiality, security, retention and deletion of personal data.
- Consider the location of data storage and any international transfers.
- Ensure that arrangements exist for the secure retrieval, transfer and deletion of data when contracts end.

The Data Protection Officer (DPO) and school leaders will periodically review cloud services and associated risks to ensure continued compliance with legal, operational and security requirements.

Any actual or suspected data breach involving cloud services must be reported immediately in accordance with the school's Data Breach Procedure.

## 23. Data Retention

The school will retain personal data only for as long as necessary to fulfil the purposes for which it was collected and to meet legal, statutory, safeguarding, operational and contractual requirements.

The school will maintain a Records Retention Schedule which identifies retention periods for different categories of records.

When retention periods expire, personal data will be securely deleted, destroyed or anonymised, unless there is a lawful reason for continued retention.

Paper records will be securely shredded, pulped or disposed of through an approved confidential waste process. Electronic records will be securely erased, deleted or destroyed using appropriate methods to prevent recovery.

The school may retain certain records relating to former pupils, staff, governors or volunteers where required for safeguarding, legal, historical, pension, employment or educational purposes.

Regular reviews of retained information will be undertaken to ensure compliance with legal and operational requirements.

## 24. DBS Information

The school will process Disclosure and Barring Service (DBS) information in accordance with UK GDPR, the Data Protection Act 2018 and the DBS Code of Practice.

DBS information will only be accessed by authorised individuals who require the information as part of their role.

The school will:

- Store DBS information securely.
- Restrict access to DBS information on a need-to-know basis.
- Maintain confidentiality at all times.
- Ensure that DBS information is not retained longer than is necessary.
- Dispose of DBS information securely when no longer required.

Where a DBS certificate has been presented, the school will ordinarily retain only a record of:

- The applicant's name.
- The type of check undertaken.
- The certificate number.
- The date of the check.
- The outcome of the suitability decision.

Copies of DBS certificates will not normally be retained beyond six months after a recruitment decision has been made unless there is a lawful reason for doing so.

Any third party processing DBS information on behalf of the school will be required to comply with applicable data protection legislation, confidentiality requirements and information security standards.

## 25. Monitoring and review

This policy is reviewed annually by the DPO and the headteacher.

The next scheduled review date for this policy Aug 2027