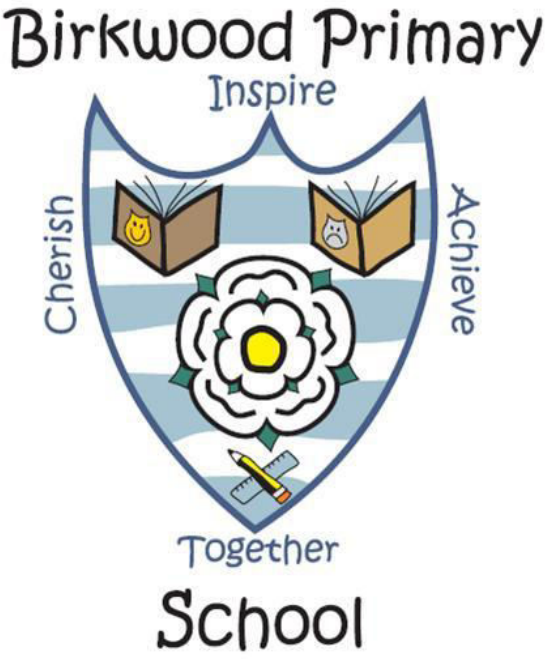


# UK-GDPR DATA PROTECTION POLICY

## REVIEWED MARCH 2022

**Statement of Intent**
Birkwood Primary School aims to ensure that all personal data collected about its staff, pupils, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with its legal obligations.

**Legal Framework**

The legal framework for this policy was formerly based on European Union legislation. Going forward, the European Union GDPR will not apply directly to UK organisations, including schools, so they will still have to follow its rules which were adopted into United Kingdom law by the UK Data Protection Act. In addition, the UK government has introduced legislation, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 which amends the DPA, merging it with the requirements of the EU GDPR; this produces what has been referred to as the 'UK-GDPR'. There may be some temporary changes to rules on transfer of personal data between the UK and the EU/EEA (European Economic Area). This policy will be amended once further clarification is in place.

- Data Protection Act (2018)
- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005

**Definitions**

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |

| | |
|---|---|
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br>Processing can be automated or manual. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

**The Data Controller**

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Headteacher.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

**Roles and Responsibilities**

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

**Governing Body**

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

**Data Protection Officer**

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and providing support and advice to the school to support the development of related policies and guidelines where applicable.

They will provide an annual report of their activities to the governing body and, where relevant, report to the body their advice and recommendations on school data protection issues.

The school's designated DPO has been appointed by the collaboration. The DPO should be the first point of contact for individuals whose data the school processes, and for the ICO. Contact

should however be made via the school and this is reflected in the school's privacy notices.
Full details of the DPO's responsibilities are set out in their job description/contract.

**Headteacher**
The headteacher acts as the representative of the data controller on a day-to-day basis.

**All staff**
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

**Data Protection Principles**

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

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up-to-date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

**Collecting Personal Data**

**Lawfulness, fairness and transparency**

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract

- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent***

** The school ensures that consent mechanisms meet the standards of the UK-GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent must therefore be a positive indication and will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is requested, a record will be kept documenting how and when consent was/was not given. Consent can be withdrawn by the individual at any time.*

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK-GDPR and Data Protection Act 2018. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

**Limitation, minimisation and accuracy**
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data through our school privacy notices.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the schools data retention policy guidelines.

*Sharing personal data*
We will not normally share personal data with anyone else, but may do so where:
- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data processing/sharing agreement (see Appendix 1) with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations

- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law and ensure that a Standard Contractual Clause (SCC) is in place.

*Subject access requests and other rights of individuals*

**Subject access requests**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Please note that during the Summer holidays, the school's post is retained by the Royal Mail until school re-opens in September. Any SAR should be emailed to d.white@birkwood.org.uk

If staff receive a subject access request they must immediately forward it to the DPO.

**Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a

request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Includes information related to a third party
- Is included in the list of exemptions in the DPA(2018)

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

A Subject Access Requests must be submitted/confirmed using the school template – see Appendix 2

**Other data protection rights of the individual**

In addition to the rights outlined above, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

*Parental requests to see the educational record*

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

*Photographs and videos*

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to parent/carers and pupils.

Uses may include:

- Within school e.g. on notice boards, the school's MIS system etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns, sporting clubs, companies who support school with additional learning opportunities
- Online on our school website
- Class and individual photos taken by the school's official photographer
- External Social Media platforms or Apps, such as Twitter

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete any photographs or video held as advised.
When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified unless the photo is of a group.

*Data protection by design and default*

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law

- Completing privacy impact assessments (see Appendix 3) where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new projects/technologies (the DPO will advise on this process).

- Integrating data protection into internal documents including this policy, any other related policies and privacy notices

- Training members of staff and governors on data protection law, this policy, any related policies and any other data protection matters. Training will be provided as part of the school's induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

- Conducting regular reviews and audits to test our privacy measures and make sure we are compliant

- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure (data audit)

*Data security and storage of records*

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals. Workstations must be locked when not in use.
- Encryption software is used to protect all portable devices and removable media, such as

laptops and USB devices

- Daily backups of data stored on the school server will be taken, tapes will be stored securely on site, a copy will also be taken off site daily
- Emails containing personal, sensitive or confidential information are sent using Outlook encryption
- Consideration will be given to whether or not emails to a number of recipients should be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Procedures are in place to manage the removal of school information e.g. email access from mobile devices that are reported missing
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of loss/theft.
- Where paper based personal data is taken off site e.g. on school trips, the information held will be kept to a minimum e.g. first names only. Contact numbers will not be taken unless absolutely necessary, out of hours contact will be made using the school's text messaging service.

*Disposal of records*

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

The school follows the retention schedule provided by the Information Records Management Society

*Personal data breaches*

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 4.

The school will speak to the DPO to evaluate the impact on data subjects. The school will undertake the following:

a. If it is a contained breach, where data has been compromised, but there has been no criminal or financial impact on the data subect(s), it will complete a Data Breach form and ensure it undertakes further training with staff.

b. If a serious breach as occurred and data has been compromised which could impact on the data freedoms of individuals, it will contact the ICO within 72 hours.

*Monitoring arrangements*

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when there are changes in data protection legislation or every 2 years, whichever is sooner, and will be approved by the governing body.

*Links with other policies*

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Acceptable use policy
- Photography Policy
- Retention policy

**Appendix 1**

**Data Sharing Agreement example letter**

Dear ,

As one of our service providers, we are writing to you regarding the personal information that you process on our behalf in your capacity as a website and communications provider.

You will be aware that on the 25th May 2018 the *General Data Protection Regulation (GDPR)* comes into force, superseding the existing data protection laws and introducing tighter controls and a more risk-based approach for processing personal information and protecting the rights and freedoms of individuals.

As a data Controller, Birkwood Primary has an obligation to ensure that any service provider *("Processor")* processing personal data on our behalf, abides by the principles and requirements of the GDPR and UK data protection law. We expect all Processors appointed by us to provide sufficient guarantees and evidence that the requirements of the GDPR will be met and the rights of data subjects protected.
The GDPR makes it a legal requirement to have a written contract in place whenever a Controller uses a Processor; the purpose of which is to define the business relationship and to ensure that both Controller and Processor understand their obligations, responsibilities and liabilities with regards to personal information and data protection.

Birkwood Primary School has therefore drafted the enclosed *Processor Agreement* which relates specifically to our business relationship and details the subject matter; duration; nature and purpose of the processing; the type of personal data and categories of data subject; the obligations and rights of our school as the Controller.

The agreement also outlines your responsibilities and obligations as a Processor and provides the terms for processing any personal information disclosed by our school ensuring that we both meet our Article 28 obligations.
Please could you read, complete and sign the enclosed ***Processor Agreement*** and return it to us at your earliest convenience together with evidence to demonstrate your compliance with the obligations and rights outlined in section 3 of the agreement.

Please ensure that you complete the ***schedules section***, providing full details of the organisational and technical measures taken to ensure data security and protection, and where applicable, provide details of any sub-Processor(s) used.

Completed agreements can be emailed to Rachel Cocking, School Business Manager at r.cocking@birkwood.org.uk or can be returned by post to:

Birkwood Primary School
Darfield Road
Cudworth
Barnsley
S72 8HG

Tel: 01226 710447

If you have any further questions, please do not hesitate to contact us.

Yours sincerely,

**Rachel Cocking**
School Business Manager
***enc. Processor Agreement***

## DATA PROCESSOR AGREEMENT

This data processing agreement forms part of the [contract name] ***("Principal Contract")*** and is made effective from ____ day of _____, 20___ ***between*** the undersigned parties: -

**Birkwood Primary School,** whose trading address is Darfield Road, Cudworth, Barnsley S72 8HG

***And***

**[Processor Name],** whose trading address is **[Processor Trading Address]** ***("Processor")***

### 1. Terms of Agreement

1. This agreement supplements the Principal Contract and makes legally binding provisions for compliance with the Data Protection Laws as set forth in this agreement. As per the requirements of relevant Data Protection Law, all processing of personal data by a processor on behalf of a controller, shall be governed by a contract. The terms, obligations and rights set forth in this agreement relate directly to the data processing activities and conditions laid out in Schedule 1.
2. The terms used in this agreement have the meanings as set out in the *'definitions'* part of the document

### 2. Definitions

1. In this Agreement, unless the text specifically notes otherwise, the below words shall have the following meanings: -
2. *"Consent"* of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
3. *"Data Protection Laws"* means all applicable Data Protection Laws, including the General Data Protection Regulation (GDPR) (EU 2016/679), [Data Protection Bill] and, to the extent applicable, the data protection or privacy laws of any other country
4. *"EEA"* means the European Economic Area
5. *"Effective Date"* means that date that this agreement comes into force
6. *"Personal Data"* means any information relating to an identified or identifiable natural person ('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
7. *"GDPR"* means the General Data Protection Regulation (GDPR) (EU) (2016/679)
8. *"Principal Contract"* means the main contract between the parties named in this agreement
9. *"Processing"* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
10. *"Recipient"* means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union

or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing

11. *"Third-party"* means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

12. *"Sub Processor"* means any person or entity appointed by or on behalf of the Processor to process personal data on behalf of the Controller

13. *"Supervisory authority"* means an independent public authority which is established by a Member State pursuant to Article 51 of the *"GDPR"*

**3. Obligations and Rights of the Processor**

1. The Processor shall comply with the relevant Data Protection Laws and must: -
   a. only act on the written instructions of the Controller
   b. ensure that people processing the data are subject to a duty of confidence
   c. ensure that any natural person acting under their authority who has access to personal data, does not process that data except on instructions from the Controller
   d. use its best endeavours to safeguard and protect all personal data from unauthorised or unlawful processing, including *(but not limited to)* accidental loss, destruction or damage and will ensure the security of processing through the demonstration and implementation of appropriate technical and organisational measures as specified in Schedule 1 of this agreement
   e. ensure that all processing meets the requirements of the GDPR and related Data Protection Laws and is in accordance with the Data Protection Principles
   f. ensure that where a Sub-Processor is used, they: -
      i. only engage a Sub-Processor with the prior consent of the data controller
      ii. inform the controller of any intended changes concerning the addition or replacement of Sub-Processors
      iii. they implement a written contract containing the same data protection obligations as set out in this agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Data Protection Laws
      iv. understand that where any Sub-Processor is used on their behalf, that any failure on the part of the sub-processor to comply with the Data Protection Laws or the relevant data processing agreement, the initial processor remains fully liable to the controller for the performance of the Sub-Processor's obligations
   g. assist the Controller in providing subject access and allowing data subjects to exercise their rights under the Data Protection Laws
   h. assist the Controller in meeting its data protection obligations in relation to: -
      i. the security of processing
      ii. data protection impact assessments
      iii. the investigation and notification of personal data breaches
   i. delete or return all personal data to the Controller as requested at the end of the contract
   j. make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the relevant Data Protection Laws and allow for, and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller
   k. tell the Controller immediately if they have done something (*or are asked to do something*) infringing the GDPR or other Data Protection Law of the EU or a member state
   l. co-operate with supervisory authorities in accordance with GDPR Article 31
   m. notify the Controller of any personal data breaches in accordance with GDPR Article 33
   n. where applicable, employ a Data Protection Officer if required
   o. where applicable, appoint *(in writing)* a representative within the EU if required in accordance with GDPR Article 27
2. Nothing within this agreement relieves the processor of their own direct responsibilities,

obligations and liabilities under the General Data Protection Regulation *(GDPR)* or other Data Protection Laws.

3. The Processor is responsible for ensuring that each of its employees, agents, subcontractors or vendors are made aware of its obligations regarding the security and protection of the personal data and the terms set out in this agreement.

4. The Processor shall maintain induction and training programs that adequately reflect the Data Protection Law requirements and regulations, and ensure that all employees are afforded the time, resources and budget to undertake such training on a regular basis.

5. Any transfers of personal data to a third country or an international organisation shall only be carried out on documented instructions from the controller; unless required to do so by Union or Member State law. Where such a legal requirement exists, the Processor shall inform the Controller of that legal requirement before processing.

6. The Processor shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing: -

   a. the name and contact details of the Processor(s) and of each Controller on behalf of which the Processor is acting, and, where applicable, the data protection officer
   b. the categories of processing carried out on behalf of each Controller
   c. transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards
   d. a general description of the technical and organisational security measures referred to in Article 32(1)

7. The Processor shall maintain records of processing activities in writing, including in electronic form and shall make the record available to the supervisory authority on request

8. When assessing the appropriate level of security and the subsequent technical and operational measures, the processor shall consider the risks presented by any processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

## 4. Obligations and Rights of the Controller

1. The Controller is responsible for verifying the validity and suitability of the Processor before entering into a business relationship.

2. The Controller shall carry out adequate and appropriate onboarding and due diligence checks for all Processors, with a full assessment of the mandatory Data Protection Law requirements.

3. The Controller shall verify that the Processor has adequate and documented processes for data breaches, data retention and data transfers in place.

4. The Controller shall obtain evidence from the Processor as to the: -

   a. verification and reliability of the employees used by the Processor
   b. certificates, accreditations and policies as referred to in the [due diligence/onboarding questionnaire]
   c. technical and operational measures described in ***Schedule 1*** of this agreement
   d. procedures in place for allowing data subjects to exercise their rights, including *(but not limited to*), subject access requests, erasure & rectification procedures and restriction of processing measures

5. Where the Controller has authorised the use of any Sub-Processor by the initial Processor, the controller must verify that similar data protection agreements are in place between the initial Processor and Sub-Processor.

6. Where the Controller has authorised the use of any Sub-Processor by the initial Processor, the details of the Sub-Processor must be added to *Schedule 2* of this agreement.

## 5. Penalties & Termination

1. By signing this agreement, the Processor confirms that they understand the legal and enforcement actions that they may be subject to should they fail to uphold the agreement terms or breach the Data Protection Laws. If the processor fails to meet their obligations, they may be subject to: -

a. investigative and corrective powers of supervisory authorities under Article 58 of the GDPR
b. an administrative fine under Article 83 of the GDPR
c. a penalty under Article 84 of the GDPR
d. pay compensation under Article 82 of the GDPR

2. The Controller or Processor can terminate this agreement by [insert termination terms and notification periods].

**6. General Information**

1. [insert any other clauses or terms specific to this Processor and your business relationship]

IN WITNESS below of the parties or their duly authorised representatives have signed this agreement in accordance with all its clauses and on the day, month and year stated at the top of this agreement.

| | |
|---|---|
| Signed on behalf of the Processor: | Signed on behalf of the Controller: |
| Signed: | Signed: |
| Print Name: | Print Name: |
| Date: | Date: |
| Company Name: | Company Name: Birkwood Primary |
| Position: | Position: |

**SCHEDULE 1**

**1. Processing Details**

a. The Controller named in this agreement has appointed the Processor with regard to specific processing activity requirements. These requirements relate to **[insert subject-matter - This should be a high level, short description of what the processing is about i.e. its subject matter]**.

b. The duration of the processing is for/until **[insert duration/end date/until further notice - Clearly set out the duration of the processing including dates].**

c. The processing activities relate to **[insert the nature - Be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.]** and are for the purpose of **[insert purpose of the processing - The purpose might include, by way of examples only: employment processing, statutory obligation, recruitment assessment etc.]**.

d. The requirement for the named Processor to act on behalf of the Controller is with regard to the below type(s) of personal data and categories of data subjects: -

i. **[insert type(s) of personal data - Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]**

ii. **[insert categories of data subjects - Personal Data / Special Category Data / Child Data (If more than one category, list all) and to each category provide an explanation such as these examples: staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a** particular website **etc.]**

e. The Processor can demonstrate and provide sufficient guarantees as to the implementation of appropriate technical and organisational measures taken to ensure data security and protection: -

a. **[insert technical measures]**
b. **[insert organisational measures]**

f. The obligations and rights of the Controller and Processor are set out in section (2) and (3) of this agreement.

**SCHEDULE 2**

**1. Authorised Sub-Processors**

| SUB-PROCESSOR NAME | CONTACT DETAILS | PURPOSE OF PROCESSING | TYPE OF DATA PROCESSED | AUTHORISED BY CONTROLLER *(Signature)* |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

[Include further schedules if applicable/required by the business relationship *(i.e. contract clauses, binding corporate rules etc)*]

**Appendix 2**

**Subject Access Request Proforma**

Application to make a subject access request under Section 7 of the Data Protection Act 1998. The person who the personal data is about is known as the data subject and the person who is making the request is known as the applicant. These can of course be the same person depending on the personal data sought. The information you provide on this form will be used only for the purposes of processing your request.

**1. Details of applicant**

First Name: _____Surname: _____

Address:_____

_____

_____

Postcode: _____

Telephone: _____

Email: _____

I am the data subject (please tick)

☐ Yes – Go to section 3

☐ No – Go to section 2

**2. Details of data subject**

First Name: _____ Surname: _____

Address: _____

_____

Postcode: _____

Telephone: _____

Email: _____

**3. Details of information being requested**

Please provide a clear description of the information you are requesting including, dates, departments and/or any additional information which will enable us to locate it (continue on a

separate sheet if required).

## 4. Fee

Information will be provided free of charge unless your request is found to be repetitive or excessive. In this instance we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. If a charge is to be levied this will be notified before a request is processed.

## 5. Proof of identity/consent

Please send us copies of two documents that prove who you are.

One must be photographic (such as a valid passport or driving licence) and;

One must prove your current address (such as a recent electricity bill, or council tax bill).

Alternatively if you are in regular contact with the school, you may wish to arrange an appointment to confirm identification in person. However, proof of address will be required regardless unless collection of information will be in person also.

Please tick either:-

☐ The information requested is about myself.

☐ I am the parent/guardian requesting access to my child's personal data who is under 12 years of age. (Please note that whilst we generally only require their written consent if the child is older than 12 years of age, the Data Protection Act requires us to assess competency which is not restricted to age. Therefore in exceptional circumstances, consent may still be required)

☐ I am representing another individual

In addition to the required identification outlined above, please send us one form of identification and written permission from the person that the information is about, saying that we can give you their information. Please note that in some circumstances we may need to verify authenticity.

## 6. Declaration

I am the person named in section one of this form and the information I have supplied is accurate. I am asking for personal information held by the school about me / the named person under the provisions of Section 7 and am aware that the unlawful obtaining of persor data is an offence under Section 55 of the Data Protection Act 1998.

Signed: _____ Date: _____

Print: _____

***Office use***

| | | | |
|---|---|---|---|
| *Received date* | | *Reference* | |
| *ID required/received* | | *Received by* | |
| *Fee* | | *Proof of address* | |

| | | | |
|---|---|---|---|
| *required/received* | | *required/received* | |

**Appendix 3**

**Privacy Impact Assessment**

| |
|---|
| What is the aim of the project? |
| |
| What data will be collected? e.g. pupils, parents |
| |
| How will the data be collected? e.g. paper, electronically |
| |
| Where will the data be stored? e.g. filing cabinet, server, cloud, third party company |
| |
| How will the data be shared? LA, DfE, Third party |
| |
| How will the data be amended or deleted? |
| |
| Identified risks e.g. potential risks of losing data – subjects/school etc. |
| |

| |
|---|
| |

Signed: _____ Date: _____

**Appendix 4**

**Data breach**

| | |
|---|---|
| Date of breach | |
| Person responsible for dealing with breach | |
| Description of breach | |
| Which data subjects are involved? e.g. pupils, staff | |
| Reported by | |
| Is this high risk? Has it been reported to ICO? | |
| Date reported to data subjects? | |
| Actions taken? | |
| Lessons learned e.g. preventative actions | |
| Notes | |

| | |
|---|---|
| | |
| Actions approved by/date | |

Signed by: _____ Date completed: _____

Position: _____

This data protection policy has been approved and adopted by the Governing Body on

_____ Signed by: _____

*Chair of Governors*

## Monitoring and Review

The Governing Body reviews this policy every year. The Governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the governing body receives recommendations on how the policy might be improved.

This policy will be reviewed in March 2024

Signed _____Headteacher Date _____

Signed _____Chair of Governors Date _____