

Data Protection Policy

For Data Subjects

Ryders Green Primary School

|  |  |
| --- | --- |
| Date of last review: | September 2019 |
| Date of this review: | September 2022 |
| Date of next review: | September 2024 |

**Contents**

|  |  |
| --- | --- |
| **Policy Section** | **Page Number** |
| Purpose |  |
| Introduction |  |
| Definitions and Common Terminology |  |
| Data Protection Principles and How Ryders Green Primary Complies |  |
| Roles and Responsibilities |  |
| Data Processing Measures |  |
| Collecting/Use of Personal Data |  |
| Subject Access Requests and other rights of individuals |  |
| Children and Subject Access Requests |  |
| Responding to a Subject Access Request |  |
| Parental Requests to see the educational record |  |
| Complaints to the Information Commissioner |  |
| Photographs and Videos |  |
| CCTV |  |
| A Data Subjects Rights |  |
| Destruction of Records |  |
| Data Breaches |  |
| Training |  |
| Contact Details |  |
| Monitoring Arrangements |  |

**1. Purpose**

*Ryders Green Primary School* Data Protection Policy is intended to ensure that personal information is dealt with securely and in accordance with the Data Protection Act 2018, EU General Data Protection Regulation (GDPR). It will apply to all data held by the school regardless of the way it is used, recorded and stored and whether it is held by the school in paper files or electronic form.

**2.** **Introduction**

Ryders Green Primary School collect and use certain types of personal information about pupils, parents, staff and other individuals who come into contact with the school in order to provide education and other associated functions. Our school is required by law to collect and use certain types of information to comply with statutory obligations related to education, safeguarding and employment, and this policy is intended to ensure that personal information is dealt with securely and in accordance with the GDPR. The GDPR applies to all electronic and manual data files

This policy will apply to any member of staff in the school who process personally identifiable information. Ryders Green Primary School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR. Ryders Green Primary School will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

This policy will be updated when amendments to the data protection legislation are made or to reflect best practice where necessary. The policy will be reviewed every 2 years.

**3. Definitions and Common Terminology**

*Data Controller* – a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and, means of the processing of personal data.

*Data Processor* – a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller.

*Data Subject –* an identified or identifiable living individual whose personal data is held or processed.

*Personally Identifiable Information* – any information relating to an identified or identifiable, living individual.

*Special Categories of Personal Data* – personal data which is more sensitive and so needs more protection, including information about an individuals, racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetics; biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes, Health – physical or mental, sex life or sexual orientation.

*Data Protection Officer* – a person who is tasked with helping to protect PII, and helping an organisation to meet the GDPR compliance requirements, does not hold ultimate accountability for compliance.

*Subject Access Request* – a right that a person has to obtain a copy of information held about them by the organisation.

*Data Breach* – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

*ICO* – Information Commissioners Office (Supervising Authority in the UK)

**4. Data Protection Principles and How** Ryders Green Primary School **Complies**

As the Data Controller, Ryders Green Primary School processes personal data in line with the GDPR sets of guiding principles as follows:

|  |  |
| --- | --- |
| **Data Protection Principles** | **How the School Will Comply** |
| Legality, Transparency and Fairness  *Personal data will only be processed by the school, where it is able to demonstrate that it has a ‘Lawful basis’ for the processing activity* | A data mapping document identifies all data processed by the school to monitor and review the ‘lawful basis’ for collecting, processing, sharing, storing and destroying data.  A Privacy Notice for pupils, parents/carers, staff and visitors to school is readily available and includes all details of the data collected. |
| Purpose Limitation  *Personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.* | A data mapping document will identify the purposes for which processing will take place, the description of the categories of individuals and personal data, the categories of recipients of the data (eg Third party organisations who the school shares the data with. Retention schedules for the personal data will also be noted. |
| Data Minimisation  *The personal data must be ‘Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’* | Data collection forms will be regularly reviewed to ensure information is appropriate and not excessive.  Data required by teaching staff will be provided only for the purpose it is required to ensure information used is minimal. |
| Accuracy  *All reasonable steps will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.* | Data will be regularly checked to ensure it is as accurate as possible through a variety of measures:   * Issue data collection forms on an annual basis to parents/carers to check and amend data held. * Parent light App (if used by the school) * Reminders on school newsletters * During Parents Evening * Pupil progress meetings * School Comms * Tapestry |
| Storage Limitation  *Personal data shall be kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.* | Retention periods for various data held in the school are recorded within the data mapping document. The school refer to the Information Record Management Toolkit to establish appropriate retention periods and data is archived and destroyed as set out in these guidelines. |
| Integrity and Confidential (Security)  *Personal data will be processed in a manner, which 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* | Electronic devices, such as computers, laptops, ipads, etc are password protected. Passwords are a minimum of 8 characters and contain a mixture of upper case, lower case letters and numbers.  Passwords are changed on a regular basis  Computers are locked when not in use.  Secure transmission of data: Secure password protected exchange sites are used to transfer data  Clear desk policy is in place around school.  Paper based data is stored in secure lockable cabinets.  Offices around school are locked at all times.  Access to the school site is secure with an intercom secure system in operation.  School to include other measures in place – details from the data walk report may be used if required. |
| Accountability  Ryders Green Primary School *as data controller will be able to demonstrate compliance with the previous principles.* | A data protection officer is appointed.  A data protection lead is first point of contact.  Ryders Green Primary School has clear procedures in place for handling a data breach and a Subject Access Request  Third party agreement/assurances are in place for all data shared with such organisations who process data on behalf of the school.  School staff are GDPR trained on an annual basis.  Regular Data Audits and reviews will be undertaken to check the robustness of processes and systems for continued GDPR compliance |

**4. 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 Board**

The governing board 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 developing related policies and guidelines where applicable.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Sue Courtney-Donavan is contactable via [gdpr@sips.co.uk](mailto:gdpr@sips.co.uk)

For day to day data protection queries please contact [contactus@rydersgreen.sandwell.sch.uk](mailto:contactus@rydersgreen.sandwell.sch.uk) alternatively email [ict@rydersgreen.sandwell.sch.uk](mailto:ict@rydersgreen.sandwell.sch.uk).

**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

**6. Data Processing Measures**

The school have put measures in place to show that data protection requirements are integrated into all data processing activities. These include:

* appointment of a suitably qualified Data Protection Officer (DPO) which is provided to the school by SIPS Education, and are contactable via [gdpr@sips.co.uk](mailto:gdpr@sips.co.uk) or 0121 296 3000
* maintaining up to date, data mapping records to ensure that processing of personal data for a specific purpose is undertaken in line with the data protection principles as set out in GDPR.
* 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 data protection impact assessments where the school’s processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
* Integrating data protection into internal documents including this policy, any related policies and privacy notices
* Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
* Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
* Where the school is introducing new technologies or it is considered that the processing of personal data presents a high risk to the rights and freedoms of individuals, data protection impact assessments will be completed by the relevant staff in liaison with the Data Protection Lead within the school
* Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
* 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 (via our privacy notices)
  + For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

**7. Collecting/Use of Personal Data**

**Lawfulness, Fairness and Transparency**

We will only process personal data where we have one of the 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 or another person i.e. to protect someone’s life
* The data needs o be processed so that the school as a public authority, can **perform a task in the public interest or exercise its official authority**
* The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

* The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
* The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
* The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
* The data has already been made **manifestly public** by the individual
* The data needs to be processed for the establishment, exercise or defence of **legal claims**
* The data needs to be processed for reasons of **substantial public interest** as defined in legislation
* The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
* The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
* The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

* The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
* The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
* The data has already been made **manifestly public** by the individual
* The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
* The data needs to be processed for reasons of **substantial public interest** as defined in legislation

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Ryders Green Primary School process personal data on pupils, staff and visitors. Personal data for each individual will be processed in accordance with the GDPR principles.

In accordance with the principle of transparency, the school has developed and will maintain privacy notices for different categories of data subject. These outline the categories of data captured, the purpose of processing and if the information is shared with third parties.

Our data mapping document informs the content of our privacy notices, which can be found on our website or within the shared area of the school’s electronic system for staff.

Privacy notices have been drafted for the following categories of data subjects:

* Pupils
* Parents/carers
* Staff and Volunteers
* Visitors and contractors
* School Governors

**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.

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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 school’s record retention schedule

**Sharing Personal Data**

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with data protection law.

**8. 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 both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

As a school we have also considered that parents/carers only photograph their own child or seek additional consent from parents\carers of all whose children are involved.

We will obtain written consent from parents\carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don’t need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Where the school takes photographs and videos, uses may include:

* Within school on notice boards and in school newsletter, brochures etc.
* Outside of school by external agencies such as the school photographer, newspapers, campaigns.
* Online on our school social media sites (Twitter/Facebook) and the website.

In order to do this, we will obtain written consent from parents / carers before we take photographs or videos of your child. We will do this at the start of every term. When we seek your consent, we will clearly explain how the photographs and/or videos are to be used.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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.

**9. CCTV**

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the code of practice for the use of CCTV

We do not need to ask individuals’ permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to contactus@rydersgreen.sandwell.sch.uk.

**10. A Data Subjects Rights**

Under the GDPR, data subjects have the following rights with regards to their personal information, as follows:

1. Right to be informed about the collection and the use of their personal data
2. Right of access personal data and supplementary information
3. Right to have inaccurate personal data rectified, or completed if it is incomplete
4. Right to erasure (to be forgotten) in certain circumstances
5. Right to restrict processing in certain circumstances
6. Right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across difference services.
7. Right to object to processing in certain circumstances
8. Rights in relation to automated decision making and profiling.
9. Right to withdraw consent at any time (where relevant)
10. Right to complain to the Information Commissioner

Individuals should submit any request to exercise these rights to the Data Protection Lead in school. If staff receive such a request, they will immediately forward it to the Data Protection Lead, who will liaise with the Data Protection officer as necessary.

**11. Subject Access Requests and other rights of individuals**

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 purpose 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
* Where relevant, the existence of the right to request rectification, erasure or restrictions, or to object to such processing
* The right to lodge a complaint with the ICO or another supervisory authority
* The source of the data, if not the individual
* The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

* Name of individual
* Correspondence address
* Contact number and email address
* Details of the information requested If staff receive a subject access request in any form they must immediately forward it to the DPO.

**12.Children and Subject Access Requests**

It is important to bear in mind that a child’s personal data is just that – their data – and does not belong to their parent / carer. As such, if a parent or carer wishes to make a subject access request for data relating to their child, the pupil need to have given their consent dependent on their age and level of understanding.

The age of 13 is used as a guide to determining when a child is generally likely to be mature enough to understand their rights, and accordingly any requests for their personal data from this age onwards would generally be expected to come from the child themselves.

For children below this age, it is less likely that they will fully understand the implications of SARs, and so it would normally be acceptable for the request to come from the parent / carer.

However, both of the situations above are used as a guide only, and each request (and requestor) will be judged on an individual case by case basis.

Subject access requests can be submitted in any form to any member of staff within the school. However, the school may contact the requester for more details in order for the school to respond to requests appropriately. If staff receive a subject access request in any form they will forward to the data protection lead within the school immediately. The data protection officer will also be advised to ensure appropriate support is provided to the school to fulfil the request.

Parents can also contact the data protection lead within the school to make a subject access request.

Information about how to make a Subject Access Request or for more details can be obtained from the Data Protection Lead within the school. Alternatively, see Appendix A for completion if you wish to submit a Subject Access Request now.

**13.Responding to a Subject Access Request**

When responding to requests, the school may:

* contact the individual via telephone to confirm the request has been made by them
* ask the individual to provide further details so that the school can verify and confirm the data required.
* request 2 forms of identification of the individual. Proof of address will also be verified.
* If a third party is requesting data, written authority or a power of attorney will be verified.

Requests will be responded to within 1 calendar month from receipt of the request. However, if additional information is required in order for the school to fulfil the request the response period will be from receipt of all information obtained. This includes receipt of proof of identity and proof of address where relevant.

Based on the complexity of the request and in line with Article 12 (3) GDPR, the timeframe in which to respond to a Subject Access Request may be extended up to 3 calendar months if required. In such instances the school will liaise with the Data Protection Officer and liaise with the requester to advise of the response time or any delays at the earliest opportunity.

Data provided to the requester may contain details of other individuals and therefore such data will be redacted (blanked out) to protect those individuals’ identity and personal data. Details contained within the documents will pertain to the appropriate individual only.

When responding to the request, the school may decide against disclosing information for a variety of reasons, including if it;

* would have an adverse affect on the rights and freedom of others
* information that might cause serious harm to the physical or mental health of the pupil or another individual;
* information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child’s best interests;
* information contained in adoption and parental order records;
* certain information which may be used in legal proceedings;
* would include personal data relating to another individual, where; the school cannot sufficiently anonymise the data to protect that individual’s rights’, we do not have their consent to release that individuals’ data, and it would be unreasonable to proceed without such consent.

If a request is determined to be ‘unfounded or excessive, the school has the right to refuse the request, or in some cases, charge a reasonable fee to cover the administrative costs of responding to the request.

If the school refuses a request they will inform the individual of the reasons why, and advise them of their right to complain to the ICO, if they wish to do so.

Other Data Protection Rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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 (in certain circumstances)
* Prevent use of their personal data for direct marketing
* Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
* Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
* 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 or Data Protection School Lead.

**14.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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

**15. Complaints to the Information Commissioner**

If you are dissatisfied with the way the school have handled your request and want to make a complaint, you may write to the Information Commissioner, who is an independent regulator. Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.

The Information Commissioner can be contacted at:

Information Commissioners Office, Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF Tel: 0303 123 1113

Website: [https://ico.org.uk](https://ico.org.uk/)

**16. Destruction of Records**

Personal data that is no longer required either due to it being out of date, inaccurate or in line with the school retention policy, will be disposed of securely.

The school will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the schools behalf. If we do so, a third party assurance will be obtained to provide school with sufficient guarantees that the company complies with data protection law.

**17. Data Breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches. The school has robust procedures in place to deal with any personal data breach and will notify the ICO where we are legally required to do so. Data subjects will be notified in instances where the rights and freedoms of such individuals has been compromised. The school will work with their Data Protection Officer to address a breach and school processes will be reviewed to mitigate risks if it is appropriate to do so.

**18. Training**

All staff and governors are provided with data protection training on an annual basis or more regularly where there are changes to legislation guidance or school processes. Training is also part of the induction process for new employees to the school.

**19. Contact Details**

If you wish to make a Subject Access Request (see point 12 and/or appendix A) or have general queries in relation to data protection within school, these should be directed to the Data Protection Lead within the school.

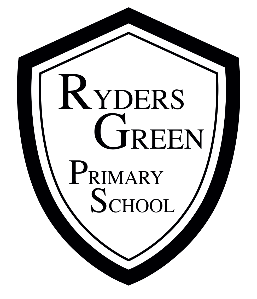
In the first instance concerns, questions or complaints, can be discussed with the Data Protection Officer at [gdpr@sips.co.uk](mailto:gdpr@sips.co.uk) or telephone number 0121 296 3000. This would include situations where there are concerns about the way a Subject Access Request or a data breach has been addressed or the robustness of policy or procedures within school in relation to Data Protection.

If you remain dissatisfied with the assistance that you have received or if you do not feel your subject access request has been dealt with appropriately or you have concerns with regards to a possible breach you can make a formal complaint to the Information Commissioners Office. This can be done via the website at [www.ico.org.uk](http://www.ico.org.uk). Telephone: 0303 123 1113 or in writing to: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A

**20. Monitoring Arrangements**

The DPO is responsible for monitoring and reviewing this policy with the school lead.

This policy will be reviewed every **2 years** and shared with the full governing board.



Appendix A - Subject Access Request Form

|  |  |
| --- | --- |
| Name |  |
| Contact Address |  |
| Contact Telephone Number |  |
| Name of pupil, data is required for |  |
| Pupils Date of Birth |  |

|  |
| --- |
| To ensure a timely response, please provide as much detail as possible about the data you require. |
|  |

Identification requirements - In order for data to be provided and to satisfy all parties that data is being shared with appropriate persons, Ryders Green Primary School will require identification of the requester, including proof of address.

If you are a third-party requesting data of an individual, written authority from the parent/pupil will be required. Where a power of attorney is in place, evidence of this will be requested prior to the release of data.

Response times - Upon receipt of the completed Subject Access Request and all information required to fulfil the request, Ryders Green Primary School will provide a response to you within 30 calendar days in line with GDPR. Should a request be deemed complex, the school will advise you of this and provide a response period, which can be up to 3 calendar months.

Please return the request to Ryders Green Primary School, Angela Johal DPL, Claypit Lane, West Bromwich, B70 9UJ. Email: [contactus@rydersgreen.sandwell.sch.uk](mailto:contactus@rydersgreen.sandwell.sch.uk) or contact on 0121 553 0658.

Signed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_