**RUSSELL LOWER SCHOOL**

**Data Protection Policy**

**Summer 2018**

**Review: Summer 2020**

Russell Lower Schoolcollects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. We are required to hold and use this personal data to comply with the Statutory Framework for the Early Years Foundation Stage, Ofsted, Department for Education and the local authority.

The School, as Data Controller, is registered with the Information Commissioner’s Office (ICO) detailing the information held and its use. These details are then available on the ICO’s website. The School has appointed the Office Manager as Data Protection Officer (DPO) who has overall responsibility for the day-to-day implementation of this policy.

The School’s Privacy Notice, which summarises the information held on individuals, why it is held and the other parties to whom it may be passed on, is published on the school’s website.

**Purpose**

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

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

**Data Protection Principles**

Russell Lower School shall comply with the six data protection principles as laid down in the GDPR (2018):

* Personal data shall be processed fairly, lawfully and in a transparent manner;
* Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
* Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose, to ensure data minimisation;
* Personal data shall be accurate and, where necessary, kept up to date;
* Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
* Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures to ensure the integrity and confidentiality of the data;

In addition, personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

**General Statement**

Russell Lower School is committed to maintaining the above principles at all times. Therefore the school will:

* Make clear why the information is being collected when it is collected
* Make clear when information is shared, and why and with whom it is shared
* Check the quality and the accuracy of the information it holds on an annual basis
* Have a review plan in place to ensure that information is not retained for longer than is necessary
* Ensure that when obsolete information is destroyed that it is done so appropriately and securely
* Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded. Electronic storage of such material will be password protected (firewall and virus protection software are in place), and paper copies of personal data will be held in locked secure cabinets. For any records stored using an online digital solution, the school will ensure due diligence has been carried out to ensure the school is compliant with GDPR.
* Share information with others only when it is necessary and legally appropriate to do so
* Set out clear procedures (See Appendix 1) for responding to requests for access to personal information, known as Subject Access Requests (SARs)
* Report any breaches of the GDPR in accordance with this policy
* Ensure our staff are aware of, and understand, our policies and procedures

**Lawful basis for processing data**

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) must be selected:

* Explicit **consent** is heldfor the individual’s data to be processed for a specific purpose; the consent is informed, unambiguous and freely given
* The processing is necessary for the performance of a **contract** to which the data subject is party, or is necessary for the purpose of taking steps with regard to entering into a contract with the individual, at their request
* The processing is necessary for the performance of a **legal obligation** to which we are subject
* The processing is necessary to protect the **vital interests** of the individual or another
* The processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the school
* The processing is necessary for the purposes of the **legitimate interests** of the school or by a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

The decision as to which lawful basis applies must be documented, and should be approved by the DPO. The school’s privacy notice(s) will inform data subjects (or their parents) of the lawful basis for processing their data, as well as the intended purpose.

**Types of personal data processed by the School**

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents, staff and other individuals, such as visitors, as part of its operation, including, by way of example:

* Names, addresses, telephone numbers, email addresses and other contact details
* Bank details and other financial information, e.g. about parents who pay fees to the School
* Employment history, information relating to career progression, information relating to DBS checks for staff
* Past, present and prospective pupils’ academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks
* Where appropriate, information about individuals’ health, and contact details for their next of kin
* References given or received by the School about pupils and staff, and information provided by previous educational establishments and/or other professionals or organisations working with pupils;
* Images of pupils (and occasionally other individuals) engaging in School activities, and images captured by the School's CCTV system (in accordance with the School's policy on taking, storing and using images of children)
* Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However in some cases personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that individual), or collected from publicly available resources

**Sensitive personal data**

The School may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the School with the explicit consent of the appropriate individual, or unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work) or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

**Use of personal data by the School**

The School will use (and where appropriate share with third parties such as CBC, Ofsted, DfE, other schools) personal data about individuals for a number of purposes as part of its operations, including as follows:

* For the purposes of pupil and staff selection and to confirm the identity of prospective staff, pupils and their parents
* To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils’ progress and educational needs; and maintaining relationships with the School community
* For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the School's performance;
* To give and receive information and references about past, current and prospective pupils and staff, including relating to outstanding fees or payment history, to/from any educational institution that the pupil has attended or where it is proposed they attend
* To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School
* To safeguard pupils’ welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips;
* To monitor (as appropriate) use of the School’s IT and communications systems in accordance with the School's Computing and Acceptable Use and E-safety Policies
* To make use of photographic images of pupils in School publications and on the School website in accordance with the School’s policy on taking, storing and using images of children
* For security purposes, and for regulatory and legal purposes (for example safeguarding and child protection and health and safety) and to comply with its legal obligations; and
* Where otherwise reasonably necessary for the School’s purposes, including to obtain appropriate professional advice and insurance for the School

Security of Personal Data

The School will ensure that measures are taken to safeguard personal data and privacy in accordance with the General Data Protection Regulation (GDPR). Everyone connected with the school has a personal responsibility to ensure that any information of a personal or sensitive nature, to which he/she has access during his/her work, is protected from unauthorised access and disclosure. All staff will be made aware of this Policy and their duties under the GDPR. The 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 must follow the School’s Acceptable User Policy, which should be referred to for further details on security of the School’s IT systems.

**Rights of individuals**

The School has an obligation to comply with the rights of individuals under the law and takes these rights seriously. Where individuals make requests under these rights, the school will always respond within one month of the receipt of the request.

**1. Right to be informed**

* The school provides privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
* The school keeps a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

**2. Right of access**

* The school enables individuals to access their personal data and supplementary information, as described in the ‘**Subject Access Requests’** section.
* The school ensures individuals are aware of and can verify the lawfulness of the processing activities

**3. Right to rectification**

* Where any request for rectification is received, it should be sent to the DPO within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and at the latest within one month and the individual notified.
* Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.
* An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

**4. Right to erasure**

Individuals have the right to have their personal data erased if:

* The personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed it;
* Where consent is withdrawn
* Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
* The personal data was unlawfully processed or otherwise breached data protection laws
* To comply with a legal obligation
* The processing relates to data provided by a child

The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

**5. Right to restrict processing**

In the following circumstances, processing of an individual’s personal data may be restricted:

* where the accuracy of data has been contested, during the period when the School is attempting to verify the accuracy of the data;
* where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
* where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;
* where an individual has objected to the school processing their data and the school is considering whether their legitimate grounds override those of the individual

Where processing is restricted, the data will still be stored. Once a decision on the accuracy of the data, or whether the School’s legitimate grounds override those of the individual, has been made, the school may decide to lift the restriction. If this is the case, the individual will be informed of this decision before the restriction is lifted.

**6. Right to data portability**

If an individual wants to send their personal data to another organisation they have a right to request that the School provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the School is processing the information on the basis of consent or performance of a contract and the processing is done by automated means, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the DPO and the DPO will review and revert as necessary.

**7. The right to object**

Individuals have the right to object to their data being used on grounds relating to their particular situation. A decision regarding the objection will be made by the DPO within one month of its receipt. Consideration will be given to:

* whether the legitimate grounds for processing override the interests, rights and freedoms of the individual.
* the processing relates to the establishment, exercise or defence of legal claims.

**8. Rights in relation to automated decision making and profiling**

The school respects the rights of individuals in relation to automated decision making and profiling.

Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention. We would only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

* It is necessary for the entry into or performance of a contract.
* Based on the individual’s explicit consent.
* Otherwise authorised by law.

In these circumstances, we will:

* Give individuals detailed information about the automated processing.
* Offer simple ways for them to request human intervention or challenge any decision about them.
* Carry out regular checks and user-testing to ensure our systems are working as intended.

**Subject Access Requests**

Anybody who makes a request to see any personal information held about them by the School is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

All requests should be sent to the DPO within 24 hours of receipt, and must be dealt with in full without delay within one month of receipt. If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. The DPO will make the decision whether an extension is necessary.

No charge will be made for providing the information, unless the request is substantial or duplicate copies are requested, in which case a reasonable charge will be made to cover administrative costs.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information.

A log of subject access requests will be kept by the DPO

**See Appendix 1 for Subject Access Request Procedure.**

**Reporting data breaches**

Any breach of this policy or of data protection laws must be reported as soon as it is discovered, to the DPO. This allows the DPO to:

* Investigate the failure, to establish the extent of the breach and the consequent risks to the data subjects
* Take remedial steps if necessary to mitigate the risk
* Maintain a register of compliance failures
* Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

If a breach has to be reported to the ICO, this must be done within 72 hours of the discovery of the breach. The ICO will be provided with the following:

* Details of the breach, including the volume of data at risk, and the number and categories of data subjects;
* The contact point for any enquiries
* The likely consequences of the breach;
* Measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the DPO shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

* The nature of the breach;
* Who to contact with any questions;
* Measures taken to mitigate any risks.

The Data Protection Officer (DPO) shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Governing Body and a decision made about implementation of those recommendations.

**Accountability and transparency**

The School will keep a written record of processing activities to include:

* The name and details of individuals or roles that carry out the processing
* The purposes of the processing
* The lawful basis for processing
* A description of the categories of individuals and categories of personal data
* Categories of recipients of personal data
* Retention schedules
* A description of technical and organisational security measures

Where processing is likely to result in high risk to an individual’s data protection rights, a Data Protection Impact Assessment (DPIA) will be carried out to assess:

* Whether the processing is necessary and proportionate in relation to its purpose
* The risks to individuals
* What measures can be put in place to address those risks and protect personal information

When carrying out a DPIA, staff should seek the advice of the DPO and once complete, refer the finalised document to the DPO for sign off.

As part of the school’s record of processing activities the DPO will document, or link to documentation on:

* Information required for privacy notices
* Records of consent
* Controller-processor contracts
* The location of personal information
* DPIAs
* Subject Access Requests
* Records of data breaches

**Responsibilities of the Data Protection Officer**

* Keeping the board updated about data protection responsibilities, risks and issues
* Reviewing all data protection procedures and policies on a regular basis
* Arranging data protection training and advice for all staff members and those included in this policy
* Answering questions on data protection from staff, board members and other stakeholders
* Responding to individuals such as clients and employees who wish to know which data is being held on them by us
* Checking and approving with third parties that handle the company’s data any contracts or agreement regarding data processing

**Responsibilities of the IT Manager (Partnership)**

* Ensure all systems, services, software and equipment meet acceptable security standards
* Checking and scanning security hardware and software regularly to ensure it is functioning properly
* Researching third-party services, such as cloud services the company is considering using to store or process data

**Training**

The school will ensure that staff are adequately trained regarding their data protection responsibilities, specific to their role. Staff must complete all training as requested. If staff move role or change responsibilities, staff are responsible for requesting new data protection training relevant to their new role or responsibilities. Staff should contact the DPO if they require additional training on data protection matters.

**Failure to comply**

The School takes compliance with this policy very seriously. Failure to comply puts both individuals and the organisation at risk. Any failure to comply with any part of this policy may lead to disciplinary action under the school’s procedures which may result in dismissal for gross misconduct.

**Complaints**

Complaints about the above procedures should be made in writing to the DPO, who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school’s complaint procedure. Complaints which are not appropriate to be dealt with through the school’s complaint procedure can be dealt with by the Information Commissioner.

**Policy Review**

This policy will be reviewed biennially, or as required if changes are made to regulations.

**Contacts**

Any questions or concerns about anything in this policy should be referred to the DPO.

DPO: Mrs S Summerfield, Russell Lower School

ICO – Information Commission’s Office – [www.ICO.gov.uk](http://www.ICO.gov.uk) – 03031 231113

Registered address: 31 Inverness Street, London NW1 7HB

Russell Lower School ICO Registration Number: Z7244257

**Appendix 1: Subject Access Request Procedure.**

**Actioning a subject access request (SAR)**

1. Requests for information should be made to the Senior Responsible Officer/DPO. Verbal or written requests are acceptable but the school recommends that the request should be put in writing (which includes email), for clarity.

2. If the initial request does not clearly identify the information required, then further enquiries will be made.

3. The identity of the requestor must be established before the disclosure of any information and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

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

NB This list is not exhaustive.

4. Any individual has the right of access to information held about them. However, with children this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher/SRO should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

5. The school will not normally make a charge for the provision of information; however, if further copies of the data, following a request is made, or the request is substantial, a fee to cover administrative costs would be charged.

5. The response time for subject access requests, once received, is 1 calendar month. However, if the request is complex or the school has received a number of requests from the individual the response time could be extended by a further two months. The school will let the individual know within one month of receiving their request and explain why the extension is necessary.

6. The Data Protection Act 2018 allows exemptions as to the provision of some information, **therefore all information will be reviewed prior to disclosure**.

7. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

8. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

9. All files must be reviewed by the SRO/DPO before any disclosure takes place. Access will not be granted before this review has taken place.

10. If there are concerns over the disclosure of information then additional advice should be sought.

11. Information disclosed should be clear, thus any codes or technical terms will be clarified and explained.

12. The data will normally be provided in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable.

Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

**Appendix 2:**

**CCTV**

Schools/educational establishments may wish to use CCTV for a number of reasons - for example, to protect against crime and to protect pupils, staff, parents and members of the public when they are on school/educational establishment premises.

Images of people captured on CCTV where they can be easily identified are defined as personal data under the Data Protection Act 2018. This means that our school must have due regard to this document when using CCTV.

Precautions are in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to the Data Protection Act 2018 and any security precautions.

Under the Data Protection Act 2018, individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Act. If a request is received, a a copy of the images must be provided within one month of the request.

Any complaints about the operation of the CCTV system should be addressed to the Headteacher, where they will be dealt with according to the school’s standard complaints procedures, with reference to the Data Protection policy.