



Data Protection Policy

Rudyard Kipling Primary School

September 2019



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Data Protection Policy

General Statement

“Data plays a key part within a modern education system. It provides the opportunity to effectively monitor the progress of learners, it allows evaluation within evidence-based practice, and it provides the opportunity for huge efficiencies in how school life operates.

The use of data across (the education) sector and beyond has developed significantly in recent years. And so it is right that the law, processes and skillsets associated with being effective guardians of children’s data are brought up to date and fit for the modern idea.” – Neil McIvor, Chief Data Officer, DfE

At Rudyard Kipling Primary School we ensure that we use data purposefully, effectively, fairly and responsibly to ensure that our students receive the best possible educational outcomes.

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The Head teacher and Governors of this School intend to comply fully with the requirements and principles of General Data Protection Regulation (GDPR). All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Terms used in this document and in the area of Data Protection

“**processing**” - obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.

“**data subject**” - The person that the data relates to, for example John Smith the pupil, Jane Smith the teacher.

“**parent**” has the meaning given in the Education Act 2002, and includes any person having parental responsibility or care of a child.

“**personal data**” - information relating to a natural identifiable person, whether directly or indirectly – for example John Smith was born on 01/01/1990. The head teacher’s salary is £60,000.

“**special category data**” - highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information. In education, it would also be best practice to treat things like FSM, SEN, and CIN/CLA status as special category data. This is tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection.

“**(data) controller**” is the organisation who (either alone or in common with other people) determine the purpose for which, and the manner in which data are processed.

“**(data) processor**” is a person or organisation who process data on behalf of and on the orders of a controller.

“**data retention**” is how long you will hold information for to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of.



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Data Protection Officer (DPO)

Under the GDPR, each school needs to appoint a named DPO in order to be compliant. The DPO role involves advising school leadership and staff about their data obligations, monitoring compliance, managing internal data protection activities, training and conducting internal audits.

The DPO will need to advise on when data protection impact assessments are required, and be available for data protection enquiries from parents and staff. Additionally, they need to be able to report directly to the board and be the point of contact for communication with the information commissioner. The Data Protection Officer at Rudyard Kipling Primary School is Steven Chennells.

Good practice in information handling

- All data should be kept safe and made available only to those who are authorised to access it.
- When data is required by an authorised user from outside the school premises – for example, by a teacher working from home – he/she should have secure remote access to the management information system or learning platform, where this is available.
- All desktop, portable and mobile devices (including media) used to store and transmit personal information, using approved encryption software, should be protected.
- Sensitive or personal data should be deleted when it is no longer required.

Fair Obtaining and Processing (The Right To Be Informed)

Rudyard Kipling Primary School & Nursery undertakes to obtain and process data fairly and lawfully. Under the GDPR the school has the following responsibilities with regards to the collection and processing of data:

- To inform individuals about the collection and use of their personal data. This is a key transparency requirement under the GDPR
- To provide individuals with information including: the school’s purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with
- To provide privacy information to individuals at the time the school collects their personal data from them
- In circumstances where the school obtains personal data from other sources, privacy information must be provided within a reasonable period of obtaining the data and no later than one month
- To provide information to people which is concise, transparent, intelligible, easily accessible, presented using clear and plain language

Subject Access

Under the GDPR, individuals will have the right to obtain:

- Confirmation that their data is being processed.
- Access to their personal data; and other supplementary information.

The details of our policy for dealing with Subject Access Requests under GDPR is explained in our Access to Information Policy.



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Data Accuracy

Under the GDPR data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. In these circumstances the school will respond to any requests within one calendar month. If the school considers that a request is manifestly unfounded or excessive the school can request a "reasonable fee" to deal with the request; or refuse to deal with the request.

Requests for rectification can be taken verbally or in writing. In the case of verbal requests, we will record these in accordance with the verbal recording policy.

Under certain circumstances individuals have the right to have their personal data erased (‘the right to be forgotten’). Of particular relevance to the school as a data controller are the following reasons:

- The personal data is no longer necessary for the purpose which we originally collected or processed it for
- The school is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent

Under certain circumstances individuals have the right to request the restriction or suppression of their personal data (‘the right to restrict processing’). Of particular relevance to the school as a data controller are the following reasons:

- The individual contests the accuracy of their personal data and the school is in the process of verifying the accuracy of the data
- The school no longer needs the personal data but the individual needs it to be kept in order to establish, exercise or defend a legal claim

Data Adequacy and Relevance

The school only collects and processes data for the following reasons:

- We need to do so in order to safely and effectively run the school
- We are required to process by law.

New Starters and Leavers Procedure.

When new staff join the school, it is important that they are given access to the correct systems and data storage areas quickly and efficiently. Similarly, when staff leave the employment of the school, it is important that their access to data subjects’ information and the school’s systems is removed. In order to facilitate this, this business manager will add an entry to the Starters/Leavers log. This is a document securely shared on OneDrive with those who need to act on it. The document is accessible by the Business Manager, Head Teacher, DPO, ICT Teaching Assistant, School Admin and ICT Technician. When the document is updated with details of a member of staff leaving, a link on the sheet is clicked by the Business Manager. This will notify the ICT Teaching Assistant who will notify the ICT Technician. Each of the three individuals will remove the member of staff who is leaving from the systems they control (see appendix 4).



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Data Retention

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of the Business Manager to ensure that obsolete data are properly erased. See Appendix 2

Authorised Disclosures

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School’s authorised officer may need to disclose data without explicit consent for that occasion. These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.
- Pupil data disclosed to authorised recipients in respect of their child’s health, safety and welfare.
- Pupil data disclosed to parents in respect of their child’s progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the school. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LEA, are contractually bound not to disclose personal data.

Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who **need to know** the information in order to do their work. The school will not disclose anything on pupils’ records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything which suggests that they are, or have been, either the subject of or at risk of child abuse.

A **“legal disclosure”** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the school, provided that the purpose of that information has been registered.

An **“illegal disclosure”** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the School’s registered purposes.

Data Integrity/Computer Security

The school undertakes to ensure data integrity by the following methods:

Data and Rudyard Kipling Primary School & Nursery undertakes to ensure security of personal data by the following general methods:

Physical Security

Appropriate building security measures are in place, such as alarms, deadlocks and an electronic visitor management system. Only authorised persons are allowed access to the server. Printouts and confidential files are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

Each classroom has one lockable cupboard. Physical copies of personal information are to be stored in this cupboard and the cupboard kept locked when the room is unattended. Any lists of medical



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

information or other personal data will be kept on display on the inside door of the cupboard so that it is easily accessible to the teaching and support staff but is not visible to children and visitors.

Physical copies of personal data are shredded as stipulated by the data retention schedules (see appendix Shredding is either carried out in-house using a Rexel Auto Plus 200X Shredder which has a P-4 security rating (each A4 sheet is shredded into approximately 200 4x40mm pieces.)

Digital storage media (such as computer hard drives, memory sticks) will be destroyed as part of end-of life recycling by an accredited recycling service).

Logical Security

‘Sophos Endpoint Security and Control’ software is installed on all computers which have access to the school network.

Only authorised users are allowed access to the computer files. Data is categorised into different security levels and staff are given access based on the needs and responsibilities of their job (see appendix I).

Network passwords expire every 90 days with users required by the system to set up new complex passwords (minimum 8 characters including upper/lower case letters and numbers). Office 365 passwords must be changed every 60 days.

All computer workstations are set up to lock to a password screen after 10 minutes.

Computer files from the school network are backed up overnight using ‘Restor Pro’ software. The data is backed up to a secure server at Brighton and Hove City Council. SIMS, FMS and Discover information are backed up onto the school server.

Data is categorised into different security levels and staff are given access based on the needs and responsibilities of their job (see appendix I)

Supply and visiting teachers are given limited access to the school network in the form of a 'Supply Drive'. Staff are able to share lesson plans and resources here. They do not have access to the rest of the school network. Any plans shared with supply staff should only use initials when children are mentioned.

Much of the school's data is stored on SIMS.net The database is stored on the school network server and is subject to the same access safeguards as other information on the network.

Supply teachers are given a 'Supply Teacher Pack' with a unique login for the network. They are provided with a paper-based register which is added to SIMS by the admin staff.

Any laptop computers which leave the school site to facilitate home working are equipped Pangolin remote access software which allow documents on the school network to be accessed securely from home.

School documents with personal information, photographs and any other personal data should not be saved or stored on staff's home computers.

All teaching and support staff are provided with Microsoft OneDrive, a 'cloud based' storage solution and productivity suite. When working at home, plans and other documents which may include personal data must be edited and processed using the online versions of Word, Excel PowerPoint etc. This will ensure that personal data is not saved to or stored on personal computers.



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Staff may access emails using their personal mobile devices but these must be password/code protected and encrypted if a mail app is used (see IT Usage Policy).

Procedural Security

All staff will take responsibility to be familiar with this policy and be aware of their personal responsibilities in ensuring the school complies with the GDPR

Computer printouts as well as source documents containing personal data must be shredded before disposal.

Computers left unattended must be locked by pressing the keyboard's Windows key and the L key or via the Start menu.

Any queries about security of data in the school should in the first instance be referred to the Data Protection Officer.

Overall security policy for data is determined by the Head teacher and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent.

Data Breaches

In the event of an apparent breach of this policy, the Head teacher will conduct an investigation, to establish what has happened and plan the next steps. See appendix 3 for the data breach procedure.

A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

If the outcome of the investigation is that there has been a deliberate breach of this Data Protection Policy, the schools Disciplinary Procedure will be followed, with the possible outcome of dismissal.

If the outcome of the investigation shows that there has been an unintentional breach of this policy, the schools Capability Procedure will be followed.

If the Headteacher is the subject of the apparent breach, the Chair of the governing body or a governor nominated to act on the Chair's behalf will lead the investigation.

Enquiries

Information about the school's Data Protection Policy is available from the School Office and the school website. General information about the GDPR can be obtained from the Information Commissioner's Office (Helpline **0303 123 1113** or **01625 545745**, website <http://www.ico.gov.uk>).

Appendix 1: Data Access Permissions

Job Title	SLT (Drive X)	SEN (Drive Q)	Governors (Drive G)	Teachers(Drive T)	Admin (Drive J)	Personal (Drive H)	Shared (Drive S)	Pupils (Drive P)	Resources (Drive R)	Netapps (Drive N)	Supply (Drive O)	SIMS	CPOMS
							SIMS database etc						
Head/Deputy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Full	Full
SLT	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Pupil+ Parents	Full
Business Manager	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Full	Full
SENCO	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Pupil+ Parents	Full
DPO	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Pupil+ Parents	Full
Inclusion Team	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Pupil+ Parents	Full
Office Staff	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Pupil+ Parents+ staff contacts	Restricted
Teachers	No	No	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Pupil+ Parents	Restricted
Teaching Assistants	No	No	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Restricted
HLTAs	No	No	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Pupil+ Parents	Restricted
Breakfast/ After school clubs	No	No	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Restricted
Dinner Staff	No	No	No	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Restricted
Governors	No	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No
Supply Teachers	No	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No
IT Tech Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Full	No
Pupils	No	No	No	No	No	Yes	No	Yes	No	Yes	No	No	No



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Appendix 2:

Data Retention Schedule - Pupil/Parent data

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
<p>Admissions Forms</p> <p>Paper copies kept in pupil record folders</p> <p>Transferred data kept on SIMS</p>	<p>Pupil at school +1 month</p> <p>Filed in pupil record folders. Record folders passed with pupil to next school.</p>	<p>Admissions files</p> <p>Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. It is then used for some validation and cross checking of enrolment details. Once enrolled, the child’s records in SIMS become the core record. Record folders passed with pupil to next school. Admissions documents are kept to ensure that any errors on SIMS can be cross referenced with the original forms.</p>
<p>Pupil files</p> <p>Stored in filing system in school office</p>	<p>event +1 month</p> <p>Retain for the time which the pupil remains at the primary school</p>	<p>Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service</p>
<p>Personal identifiers, contacts and personal characteristics</p>	<p>event +1 month (house number and road)</p> <p>pupil at school +5 years (postcodes, names, characteristics)</p>	<p>As set out in other sections, names are needed for smooth handover to subsequent schools for up to one year. Postcode data is useful in analysing longer-term performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity. Schools may well provide references for pupils for up to 3 years after they leave, and so retaining the name in the core pupil record is important (this doesn’t mean it needs to be retained in all systems). Keeping names attached to safeguarding files for longer than this may be entirely appropriate – see safeguarding section. Characteristics form an essential part of trend analysis, and so retention is in line with those needs.</p>



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
<p>Photographs of Children - Identity management/ authentication</p> <p>Part of individual records on SIMS</p> <p>Paper copies in school kitchen and staffroom. Medical info related to photos is obscured to avoid inadvertent unauthorised viewing.</p>	<p>While pupil at school +1 month (images used for identity management)</p>	<p>Images of children are included in their SIMS record to facilitate easy identification of children. This may be required to identify children with specific dietary needs or medical/allergy issues.</p> <p>Printed pictures of children need to be included in medical ‘care packs’ so that visiting teachers are aware of children in classes with specific medical conditions, allergies etc.</p> <p>reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting.</p>
<p>Photographs of Children – Celebration and evidence of learning</p> <p>These may be stored on the school network: T:/Photos and Videos. Printed copies may be kept in evidence folders, children’s books or on display boards.</p>	<p>While pupil at school +1 year (images used for evidence and in displays in school)</p>	<p>Images of children may be used to provide evidence of learning taking place. Digital copies may be kept on the school network or stored online as part of 2Build a Profile foundation stage evidence.</p> <p>Printed copies of pictures may be glued into children’s books, kept in evidence folders by class teachers, subject coordinators and learning support staff.</p> <p>Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent captured at the outset of using the photograph.</p>
<p>Biometric data</p>	<p>event +1 month (images used in identity systems) (biometrics)</p>	<p>Biometric data (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal).</p>



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
Assessment Data	Pupil at school +1 years Data with names Pupil at school +2 to 5 years Data with names removed but other identifying information retained (gender, age, SEN etc) Pupil at school +5 years Aggregated data (no identifying information)	<p>Formative assessment data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention.</p> <p>Summative attainment is the main outcome of what children ‘attain’ in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is ‘passed on’ smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment data for 1 year after the pupil has left the school feels proportionate.</p> <p>Trend analysis is important, 3 to 5 years is often the ‘trend’ people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity.</p> <p>After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.</p>
Attendance Information Detailed information kept on SIMS Aggregated information kept on Network: J:/Attendance Paper reports (aggregated/ individual % summaries in folder in office filing cupboard)	Pupil at school +1 years Data with names Pupil at school +2 to 5 years Data with names removed but other identifying information retained (gender, age, SEN etc) Pupil at school +5 years Aggregated data (no identifying information)	<p>Attendance data probably resides in some ‘operational’ systems in schools, such as cashless catering. In these systems, the data should only be retained until the associated business processes have concluded (for example, payment of meals). The start of the next academic year once all bills are settled feels proportionate.</p> <p>Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child.</p> <p>After that period, non-identifiable summary statistics are all that is required to support longer-term trend analysis of attendance patterns.</p> <p>We noted another GDPR principle here that may apply to attendance. Under data minimisation, where ‘paper records’ capture attendance, this paper record duplicates the electronic version and is probably required once the paper has been transferred to a stable electronic format.</p>



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
Behaviour Information Kept on CPOMS system	Pupil at school +1 years Data with names Pupil at school +2 to 5 years Data with names removed but other identifying information retained (gender, age, SEN etc) Pupil at school +5 years Aggregated data (no identifying information)	This is all relevant for managing children when with at your school. 1 year allows a period of ‘handover’ to next institution with conversations supported by rich data if relevant.
Racist incident Information Paper copies of incident reports kept in Deputy Head’s office	Pupil at school +1 years Data with names Pupil at school +2 to 5 years Data with names removed but other identifying information retained (gender, age, SEN etc) Pupil at school +5 years Aggregated data (no identifying information)	This is all relevant for managing children when with at your school. 1 year allows a period of ‘handover’ to next institution with conversations supported by rich data if relevant.
Exclusion Information Overview Details on SIMS Exclusion reports and letters home kept on Network: J:/Exclusions	Pupil at school +1 years Data with names Pupil at school +2 to 5 years Data with names removed but other identifying information retained (gender, age, SEN etc) Pupil at school +5 years Aggregated data (no identifying information)	Exclusion data should be ‘passed on’ to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.
Catering and free school meal management information. Stored on SIMS and school network: J:/Free School meals	While pupil at school +1 year (meal administration) pupil at school +5 years (free school meal eligibility information)	A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically ‘one month’ may not be enough, but ‘one year’ feels enough. Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7-year record also needs to be portable with the pupil, as historic dates can be used for funding.



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
School Meals Summary Sheets	Current year + 3 years	
Trips and activities	Event +1 month (educational visitors into school) Pupils at school +5 years (financial information related to trips) Until pupil is aged 25 or older (major medical events)	Financial information related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions. If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate. Permission to go on the trip slips will contain personal data, and destroying them after the trip unless any significant incident arises is appropriate, otherwise refer to the policies above.
Trips and activities (field file)	Event +1 month	A ‘field file’ is the information that is taken on a trip by a school. This can be destroyed following the trip, once any medicines administered on the trip have been entered onto the core system. If there is a minor medical incident (for example, a medical incident dealt with by staff in the way it would be dealt with ‘within school’) on the trip, then adding it into the core system would be done.
Educational visitors into school	Event +1 month	Schools sometimes share personal data with people providing ‘educational visits’ into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.
Medication permission slips Stored in folder in School Office Medical information and administration Stored on SIMS	While medication is given +1 month (permission slips) Pupil at school +1 year (medical conditions and ongoing management) Until pupil is aged 25 or older medical incidents (with a safeguarding/behavioural or ‘duty of care’ aspect)	To support any handover work about effective management of medical conditions to a subsequent institution. Permission forms that parents sign should to be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent. Medical ‘incidents’ that have a behavioural or safeguarding angle (including the school’s duty of care) should refer to the retention periods associated with those policies.



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
Accident reporting – children	Until pupil is aged 25 or older	
Safeguarding Hard copies of documents stored in Inclusion Office until archived in school ‘boiler room’ Information recorded on SIMS to be kept on database. Electronic copies of information to be kept on server	Until pupil is aged 25 or older	All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records.
Medical Information Care Packs Medical info related to photos is obscured to avoid inadvertent unauthorised viewing.	While pupil at school +1 month	Printed pictures of children need to be included in medical ‘care packs’ so that visiting teachers are aware of children in classes with specific medical conditions, allergies etc.
Special educational needs Hard copies of documents stored in Inclusion Office until archived in school ‘boiler room’. Information recorded on SIMS to be kept on database. Electronic copies of information to be kept on server	Until pupil is aged 25 or older (taken from Schools' model disposal of records schedule 2013-16 – DfE document)	This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a “failure to provide a sufficient education” case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.



Rudyard Kipling Primary School and Nursery Data Protection Policy



'Together we will help each other to achieve our best'

Data item group	Short term (event +1 month) Medium term (pupil at school +1 year) Long term (pupil at school +5 years) Very long term (until pupil is aged 25 or older)	Justification
Records relating to the identification and collection of debt	Current financial year + 6 years	
Reports for outside agencies - where the report has been included on the case file created by the outside agency	While pupil at school	
Referral forms	While the referral is current	
Family Liaison Officers and Home School Liaison Assistants Group Registers	Current year + 2 years	



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data Retention Schedule – Staff/Governors data

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Minutes of governing body minutes					Principal Set (signed)	There may be data protection issues if the meeting is dealing with confidential issues relating to staff
Agendas for Governing body minutes					One set kept with principal Set	
Reports presented to the Governing Body			+6 years		If the minutes refer directly to individual reports then the reports should be kept permanently	There may be data protection issues if the report deals with confidential issues relating to staff
Meeting papers relating to the annual parents’ meeting held under section 33 of the Education Act 2002			<i>Date of meeting + 6 years</i>			
Records relating to complaints dealt with by the Governing Body			<i>Date of the resolution of the complaint + 6 years then review for further retention in case of contentious disputes</i>			



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Log books of activity in the school maintained by the Head Teacher			<i>Date of last entry in the book +6 years then review</i>			There may be data protection issues if the log book refers to individual pupils or members of staff. These could be of permanent historical value and should be offered to the County Archives Service if appropriate
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies		<i>+3 years then review</i>				There may be data protection issues if the minutes refers to individual pupils or members of staff
Reports created by the Head Teacher or the Management Team		<i>+3 years then review</i>				There may be data protection issues if the minutes refers to individual pupils or members of staff
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities			<i>Current academic year +6 years</i>			There may be data protection issues if the minutes refers to individual pupils or members of staff



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities		+3 years then review				There may be data protection issues if the minutes refers to individual pupils or members of staff
Professional Development Plans			Life of the plan +6 years			
School Development Plans		Life of the plan +3 years				
General file series			Current year +5 years then REVIEW			
Records relating to the creation and publication of the school brochure or prospectus		Current year +3 years				
Records relating to the creation and distribution of circulars to staff, parents or pupils	Current year +1 year					



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Newsletters and other items with a short operational use	<i>Current year +1 year</i>					
Visitors’ Books and Signing in Sheets			<i>Current year + 6 years then REVIEW</i>			
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations			<i>Current year + 6 years then REVIEW</i>			
All records leading up to the appointment of a new headteacher			<i>Date of appointment + 6 years</i>			
All records leading up to the appointment of a new member of staff – unsuccessful candidates			<i>Date of appointment of successful candidate +6 months</i>			
All records leading up to the appointment of a new member of staff – successful candidate			<i>All the relevant information should be added to the staff personal file (see below) and all other information retained for 1 year</i>			



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Pre-employment vetting information – DBS Checks	<i>If copies kept NOT be retained for more than 6 months</i>					The school does <i>not</i> have to keep copies of DBS certificates.
Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	<i>If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file</i>					<i>Where possible these should be checked and a note kept of what was seen and what has been checked.</i>
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom	<i>Where possible these documents should be added to the Staff Personal File [see below]</i>			<i>if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years.</i>		
Staff Personal File			<i>Termination of Employment +6 years</i>			
Timesheets			<i>Current year +6 years</i>			
Annual appraisal/ assessment records			<i>Current year +5 years</i>			



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Allegation of a child protection nature against a member of staff including where the allegation is unfounded				<i>Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW.</i>		<i>Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned</i>
Disciplinary - oral warning	<i>Date of warning +6 months</i>					
Disciplinary - written warning level 1	<i>Date of warning +6 months</i>					
Disciplinary - written warning level 2	<i>Date of warning +12 months</i>					
Disciplinary - Final warning	<i>Date of warning +18 months</i>					
Disciplinary - Case not found				<i>If the incident is child protection related then see above otherwise dispose of at the conclusion of the case</i>		



Rudyard Kipling Primary School and Nursery Data Protection Policy



‘Together we will help each other to achieve our best’

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
Records relating to accident/ injury at work				<i>Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied</i>		
Accident reporting - adults			<i>Date of the incident +6 years</i>			
Maternity pay records		<i>Current year +3 years</i>				<i>Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)</i>
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995			<i>Current year + 6 years</i>			
Records relating to the identification and collection of debt			<i>Current financial year + 6 years</i>			
Family Liaison Officers and Home School Liaison Assistants - Day Books		<i>Current year +2 years then review</i>				



Rudyard Kipling Primary School and Nursery Data Protection Policy



'Together we will help each other to achieve our best'

Data item group	Short term need (event +1 month)	Medium term need +3 year	Long term need +6 years	Very long term need (until pupil is aged 25 or older)	Permanent	Justification
3 Family Liaison Officers and Home School Liaison Assistants - Contact data sheets	<i>Current year then review, if contact is no longer active then destroy</i>					
Contact database entries	<i>Current year then review, if contact is no longer active then destroy</i>					

Appendix 3:

Data Protection - Data Breach Procedure for Rudyard Kipling Primary School

Policy Statement

Rudyard Kipling Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Rudyard Kipling Primary School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

The Head teacher is Mrs Joanne Smith.

The Data Protection Officer is Mr. Steven Chennells.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Rudyard Kipling Primary School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

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



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Head Teacher/DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The Head Teacher/DPO must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
4. The Head Teacher/DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.
5. The Head Teacher/DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
 - a. Attempting to recover lost equipment.
 - b. Contacting the relevant Local Authority Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).
 - c. Contacting the Brighton and Hove Local Authority Press Office and the Executive Director of Education, so that they can be prepared to handle any press enquiries.
 - d. The use of back-ups to restore lost/damaged/stolen data.
 - e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
 - f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Investigation

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

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

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.



Rudyard Kipling Primary School and Nursery Data Protection Policy

‘Together we will help each other to achieve our best’

Appendix 4

Responsibilities for removing systems access for staff leaving employment at school.

(Key: BM=Business Manager, ICTSTS=ICT Schools Traded Services (Visiting IT Technician). ITTA=IT Teaching Assistant.)

Staff Leaving Admin Checklist (Staff)	
2019-20	
Name	
Role	
Date left school	
Office 365	BM
Smoothwall form	BM
SIMS login	BM
Collect Entry fob/ID badge	BM
Network login deactivated	ICTSTS
CPOMs deactivated	BM
Remove from Email groups	ITTA
Remove Sumdog login (teachers)	ITTA
Remove G-Suite Login	ITTA
Remove from Scan to Email	ICTSTS

Change Log

May 2018

Re-written to take GDPR regulations into account

May 2019

Data Retention Schedule - Pupil/Parent data (Appendix 2) clarified and simplified

October 2019

Added ‘New Starters and Leavers Procedure’ section.