DATA PROTECTION POLICY

Date written: May 2018
Date for review: May 2020

Contents

1. Aims

Sutton Park Primary RSA Academy ("the School") aims to ensure that all personal data collected about staff, pupils, parents, carers, Governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

3. Definitions

TERM	DEFINITION
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: - Name (including initials) - Identification number -Location data -Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Some personal data is more sensitive, and therefore needs more protection, including information about an individual's: -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
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The School processes personal data relating to parents, carers, pupils, staff, Governors, visitors and others, and is therefore a Data Controller. The School is registered as a Data Controller with the ICO and renews this registration annually via the Central RSA Academies Trust.

5. Roles and responsibilities

This policy applies to **all staff** employed by the School, and to external organisations or individuals working on our behalf, including Governors, volunteers, students and contractors.

5.1 Data Protection Officer (DPO)

The School's Data Protection Officer (DPO) is responsible for:

-overseeing the implementation of this policy,
-informing and advising the School and its employees about their obligations to comply with GDPR,
-monitoring the School's compliance with data protection law,
-developing related policies and guidelines where applicable,
-acting as the first point of contact for the ICO and individuals whose data is processed by the School.

The School's DPO is the first point of contact for individuals whose data the School processes, and for the ICO.

The DPO for Sutton Park Primary RSA Academy is Teresa Kristunas who can be contacted at:

Central RSA Academies Trust
B.06 Assay Studios
141 - 143 Newhall Street
Birmingham
B3 1SF

0121 270 3117

tkristunas@centralrsaacademies.co.uk

5.2 All Staff and Governors

Staff and Governors 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 School's 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, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area,

- If there has been, or they suspect that there may have 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 protection principles

The GDPR is based on data protection principles that the School must comply with. The principles say that Personal Data must be:

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

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

7. Collecting Personal Data

7.1 Lawfulness, fairness and transparency

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

1. 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.

2. The data needs to be processed so that the School can **comply with a legal obligation.**

3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.

4. The data needs to be processed so that the School, as a public authority, can perform a task **in the public interest,** and carry out its official functions.

5. The data needs to be processed for the **legitimate interests** of the School or a third party (provided the individual's rights and freedoms are not overridden).

6. 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 which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

The School 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. When staff no longer need the personal data they hold, they must ensure it is securely deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing Personal Data

The School will not normally share personal data with anyone else, but may do so where:

-There is an issue with a pupil or parent/carer that puts the safety of our staff at risk,

-There is an issue with a pupil, parent/carer, member of staff or Governor that puts the safety of another individual or individuals at risk,

-We need to liaise with other agencies – we will seek consent as necessary before doing this,

-There is a need to share such information with a third party educational service provider (eg the providers of educational applications) in order to be able to undertake our obligation to provide education. We will always ensure that all such third-party education service providers are GDPR compliant.

-Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT and catering companies. When doing this, we will:
- Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law,

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share,
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and Government bodies where we are legally required to do so, including for:

-The prevention or detection of crime and/or fraud,
-The apprehension or prosecution of offenders,
-The assessment or collection of tax owed to HMRC,
-In connection with legal proceedings,
-Where the disclosure is required to satisfy our safeguarding obligations,
-Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and Local Authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests and other rights of individuals

9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the School holds about them. This includes:
-Confirmation that their personal data is being processed,
-Access to a copy of the data,
-The purposes of the data processing,
-The categories of personal data concerned,
-Who the data has been, or will be, shared with,
-How long the data will be stored for, or if this isn't possible, the criteria used to determine this period,
-The source of the data, if not the individual,
-Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject Access Requests must be submitted in writing, either by letter or email to the School's DPO. They should include:
-Name of individual
-Correspondence address
-Contact number and email address
-Details of the information requested

If staff or Governors receive a Subject Access Request they must **immediately** forward it to the School's DPO for their action within the required timescales.

9.2 Children and Subject Access Requests

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

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, Subject Access Requests from parents or carers of pupils in our School may be granted without the express permission of the pupil.

9.3 Responding to Subject Access Requests

When responding to Subject Access Requests, we:
-May ask the individual to provide 2 forms of identification,
-May contact the individual via phone to confirm the request was made,
-Will acknowledge receipt of the request without delay and will endeavour to respond to the request within 1 month of receipt of the request,
-In exceptional circumstances we may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month of receipt of their request, and will explain why the extension is necessary,
-Will provide the information free of charge.

We will not disclose information if it:
-Might cause serious harm to the physical or mental health of the pupil or another individual,
-Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests,
-Is contained in adoption or parental order records,
-Is given to a court in proceedings concerning the child.

A Subject Access Request may be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

If the School refuses a Subject Access Request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 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 individuals also have the right to:

-Withdraw their consent to processing at any time, where their consent is required,

-Ask us to rectify, erase or restrict processing of their Personal Data, or object to the processing of it (in certain circumstances),

-Prevent use of their personal data for direct marketing,

-Challenge processing which has been justified on the basis of public interest,

-Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them),

-Prevent processing that is likely to cause damage or distress,

-Be notified of a data breach in certain circumstances,

-Make a complaint to the ICO,

-Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the School's DPO.

If staff or Governors receive such a request, they must **immediately** forward it to the School's DPO for their action.

10. Photographs and videos

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

We will always seek parental consent for this.

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 for marketing or promotional purposes we will not accompany them with any other personal information about the child or the individual, to ensure they cannot be identified.

11. Data protection by design and default

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

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

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

-Completing 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),

-Regularly training members of staff and Governors on data protection law, this policy, any related policies and any other data protection matters. We will also keep a record of attendance at such training,

-Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant,

-Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. Data security and storage of records

The School will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

-Paper-based records and portable electronic devices, such as laptops and hard drives that contain Personal Data must be kept under lock and key securely when not in use,

-All personal data (eg pupil performance data) that is stored on portable electronic devices must be stored on an encrypted drive or device,

-Papers containing confidential personal data must not be left on office or classroom desks, on staffroom tables, pinned to publicly accessible and unsupervised notice/display boards, or left anywhere else where there is general access,

-Where personal information, such as parental contact details or a pupil's medical details, needs to be taken off site, staff must sign this information in and out from school offices,

-Passwords must be used to access School computers and laptops. Staff will be required to change their passwords at regular intervals and must not under any circumstances reveal their password,

-Encryption must be used to protect all portable devices and removable media, such as USB devices,

-Where we need to share personal data with a third party, we will carry out due diligence and take reasonable steps to ensure such personal data is stored securely and is adequately protected.

13. Data Retention and Disposal of records

The School will have due regard to the Information and Records Management Society (IRMS) "Information Management Toolkit for Schools" when deciding how long to retain personal data and information.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records, and overwrite, delete or archive electronic files.

We may elect to use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. Personal Data Breaches

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

In the unlikely event of a suspected or actual data breach, we will follow the procedure set out in Appendix 1.

We will report any data breach, or suspected data breach, to the ICO within 72 hours of becoming aware of the breach or suspected breach. Such breaches may include, but are not limited to:

-A non-anonymised dataset being published on the School website which shows information about pupils eligible for the pupil premium,

-Safeguarding information being made available to an unauthorised person,

-The theft or loss of a School laptop containing non-encrypted personal data about pupils.

15. Training

All staff and Governors will be provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development for staff and Governors where changes to legislation, guidance or the School's processes make it necessary.

16. Monitoring arrangements

The School's DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years, or more frequently if such a review is deemed necessary.

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

-On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the School's DPO

-The School's DPO will investigate the report and determine whether a breach has occurred. To decide, the School's DPO will consider whether Personal Data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

-The School's DPO will alert the Senior Leadership Team and the Chair of Governors to discuss the management of the breach.

-The School's DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

-The School's DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

-The School's DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the School's DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the School's DPO must notify the ICO.

-The School's DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach.

-Where the ICO must be notified, the School's DPO will do this via the 'report a breach' page of the ICO website within 72 hours of being notified of the breach or suspected breach. As required, the School's DPO will set out:

- A description of the nature of the Personal Data breach including, where possible:

-The categories and approximate number of individuals concerned.

-The categories and approximate number of Personal Data records concerned.

- The name and contact details of the School's DPO.

- A description of the likely consequences of the personal data breach.

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

-If all the above details are not yet known, the School's DPO will report as much as they can within 72 hours of being notified of the breach or suspected breach. The report will explain that there is a delay, the reasons why, and when the School's DPO expects to have further information. The School's DPO will submit the remaining information as soon as possible.

-The School's DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the School's DPO.

- A description of the likely consequences of the Personal Data Breach.

- A description of the measures that have been, or will be, taken to deal with the Data Breach and mitigate any possible adverse effects on the individual(s) concerned.

-The School's DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

-The School's DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause

- Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Actions to minimise the impact of Data Breaches

The School will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records):

-If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

- Members of staff and Governors who receive personal data sent in error must alert the sender and the School's DPO as soon as they become aware of the error.

-In any cases where the recall is unsuccessful, the School's DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

-The School's DPO will ensure a written response is received from all the individuals who received the data, confirming that they have complied with the request to delete the information and not to share, publish, save or replicate it in any way.

-The School's DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.