Data Protection Policy – May 2018

Robert Peel Primary School

Approved by:	Robert Peel Governing Body	**Date:**	14th May 2018
Last reviewed on:	14th May 2018		
Next review due by:	31st May 2020		

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected 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 expected 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.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

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 if it's your actual name It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • 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

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing board

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

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. As a school this role is untaken by the school's data manager, admin manager, the Headteacher and named GDPR Governor who have taken steps to ensure that the data held by the school is protected.

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

These individuals are also the first point of contact for individuals whose data the school processes, and for the ICO.

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

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

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

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

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.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

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

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data 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, to the Chair of Governors either by letter or email. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested
- We do not accept 3rd party requests unless consent has been given by the said individual. If staff receive a subject access request they must immediately forward it to the DPO.

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 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers

of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

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

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

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

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

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 (see section 7), individuals also have the right to:

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

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

10. Parental requests to see the educational record

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

11. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. We will gain consent for photograph and filming to take place at school events by other parents/carers. With the explicit caveat that this is for their use only and photographs or videos are not to be shared on Social Media Sites.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages
- Filming of school events like Christmas plays

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

12. 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 suitable DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, 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

13. Data security and storage of records

We 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 are kept under lock and key when not in use and are password protected
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing upper and lower case letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords every 90 days, these are not to be shared and passwords are not reused within a 12 month period.
- To protect school data staff are to restrict details saved on to their school laptops and information is saved on to the school server via VPN access. This is password protected.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E- safety policy/ICT policy/acceptable use agreement/policy on acceptable use)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

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

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

When staff leave the school or Governors term of Governance ends they will need to state through a written confirmation that they have disposed of all electronic data securely and in accordance with data protection procedures or return all data to school.

15. Personal data breaches

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

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

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

16. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy Notices
- Safeguarding Policy
- ICT Policy
- E-Safety Policy
- Acceptable Use Policies
- Home School Agreement
- Visitors & Volunteers in School Policy
- Educational Trips & Visits Policy
- Assessment Policy
- Supply, Sports & Music Staff Policy

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 DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the 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 DPO will alert the headteacher and the chair of governors
- The 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. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The 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 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 DPO must notify the ICO.

- The 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. Documented decisions are stored in a secure area on the school server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the 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 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 DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The 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 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 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 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)
- Records of all breaches will be stored on secure area on the school server.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably practical.

Actions to minimise the impact of data breaches

We 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 who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the 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 DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The 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

Details of pupil premium interventions for named children being published on the school website

- Document removed immediately
- The parents of the named children are informed
- Staff training in checking information and documents before publishing them

Non-anonymised pupil exam results or staff pay information being shared with governors

- Governors informed of the error and that information is confidential and should not be shared with any other parties
- Staff training to ensure that details of this nature are not shared to Governors

The school's cashless payment provider being hacked and parents' financial details stolen

- Contact Payment provider and establish how the breach has occurred and if it has been rectified and corrected
- Parents informed of the breach and to check bank accounts and payments and advisedto change passwords
- Re-establish compliance expectations with payment provider and issue this to parents

Preparing for the General Data Protection Regulation (GDPR)

ICO's 12 Steps		Action
Awareness	▪ To organise awareness training in order to inform all school personnel and governors. ▪ To hold refresher training for all school personnel and governors when necessary.	▪ Staff Inset training ▪ Governor training ▪ Training details added to Single Central Record ▪ Named Governor for GDPR ▪ Regular refresher as part of safeguarding training ▪ Forming part of Staff Induction and Staff Handbook
Information we hold	▪ To organise an information audit of data held on pupils, school personnel, parents, governors/trustees and suppliers.	▪ Contact all staff about data we hold on them and what happens with this data – signed consent ▪ Re-send all parents their child's information sheet with letter explaining the data we hold ▪ Resend and get signed Privacy Notices – staff, parents, Governors ▪ Resend and get signed Acceptable Use Policies ▪ New starter form ▪ Re-do all consent for existing children for photos, medication etc ▪ Lockable filing cabinets for each classroom ▪ Lockable cupboard doors in SEND Room, The Lodge and the Qube
Communicating Privacy Information	▪ To review current privacy notices and to undertake any necessary changes before the implementation of GDPR.	▪ New Privacy Notices ▪ Sent to all relevant parties and signed consent ▪ Acceptable Use Policy signed
Individuals Rights	▪ To check current procedures to ensure they cover all the rights of individuals.	▪ New Data Protection Policy

Subject Access Requests	▪ To update present procedures, to plan how to handle requests within the new one month timescale and to provide any additional information.	▪ New Data Protection Policy ▪ Senior Staff understand procedures ▪ Destroying any data which is passed the timeframes for storing ▪ Streamline recording mechanisms via Safeguarding Monitor
Lawful basis for processing personal data	▪ To review the various types of data processing that the school carries out and then identify and document the legal basis for carrying it out.	▪ Review all software used by the school which holds or processes staff and pupil data. Obtain Compliance Statements ▪ New Starter Form to be used ▪ New Data Protection Policy ▪ Produce GDPR Eco-System
Consent	▪ To review how the school seeks, obtains, records consent and consider any changes that are required.	▪ Produce GDPR Eco-System ▪ Re-do consent for holding and sharing data with staff and parents as part of Privacy Notices
Children	▪ To 'start thinking now about whether we need to put systems in place to verify individuals ages and to obtain parental or guardian consent for any data processing activity.'	▪ As part of Starter Forms ▪ As part of revisions to Pupil Information Sheets
Data Breaches	▪ To ensure the right procedures are in place to detect, report and investigate a personal data breach.	▪ New Data Protection Policy ▪ All staff to sign that they have read and understood ▪ All staff and Governors sign Acceptable Use Policies
Data Protection by Design and Data Protection Impact Assessments	▪ To consider when to begin implementation of the Privacy Impact Assessments.	▪ Completed by the Headteacher following school staff training and input – May 2018

Data Protection Officers	▪ To have in place a designated Data Protection Officer to take responsibility for data protection compliance. ▪ To assess where this role sits within the school's structure and governance arrangements.	▪ Data Protection Officer appointed ▪ Clear Job Description ▪ Governing Body standing agenda item to review ▪ School budget – GDPR Compliance financial contribution
International	▪ To determine (if the school operates internationally) under which data protection supervisory authority applies to the school.	▪ The school doesn't operate internationally

GDPR School Readiness Statement

ICO's 12 Steps	Statement	Date(s)
Awareness	We have held: ▪ awareness training for all school personnel on:	16th April 2018 4th June 2018
	▪ awareness training for all governors on:	14th May 2018
	▪ awareness training for parents on: Via Parentmail	May 2018
	▪ awareness training for suppliers on:	
Information we hold	We have undertaken an information audit of all data held on pupils, school personnel, parents, governors/trustees and suppliers on: Data Eco System and GDPR reviewed by Governing Body	14th May 2018
	From that audit we have made the following improvements: ▪ Storage of paper material in classrooms – filing cabinets ▪ Online Safeguarding Monitor purchased to reduce paperwork and store centrally ▪ Parentmail forms and consent module – reduce signed paperwork being returned to school ▪ Staff training and awareness ▪ Data Protection Officer in place ▪ School server used as central place to save all school data ▪ Increased password security on school email and laptop login ▪ Using encryption for documents and email correspondence ▪ Destroying old paper documents no longer relevant ▪ Renewing all consent for holding/processing data from staff and parents ▪ Improve storage in office areas and SEND base	May 2018
Communicating Privacy Information	We have reviewed current privacy notices and we have made the following improvements: ▪ New Privacy Notices issued to staff, parents and Governors – signed consent that it has been read and agreed to ▪ Displayed in school ▪ New Acceptable Use Policies	May 2018

Individuals Rights	We have checked current procedures to ensure they cover all the rights individuals have and we have made the following improvements: ▪ New Data Protection Policy ▪ New Privacy Notices to be issued ▪ New Starter Form	May 2018
Subject Access Requests	We have reviewed current procedures and we plan to handle new requests within the one month timescale by: ▪ Following Data Protection Policy	
Lawful basis for processing personal data	We have reviewed the various types of data processing that we carry out and we have identified and documented the legal basis for carrying it out by: ▪ Data Eco System completed ▪ Privacy Notice ▪ Data Protection Policy	May 2018
Consent	We have reviewed how we seek, obtain and record consent and we have made the following improvements: ▪ Parentmail consent module so no further paper copies required	
Children	We have in place the following system to verify the ages of individuals: ▪ Checking via SAM Admissions portal	
Data Breaches	We have in place the following procedures to detect, report and investigate a personal data breach: ▪ Data Protection Officer reviewing processes in school ▪ Data Protection Policy ▪ Data Protection Impact Assessment completed and reviewed ▪ Staff training and knowing how to report breaches ▪ Senior Staff awareness of reporting breaches	May 2018
Data Protection by Design and Data Protection Impact Assessments	We have started to implement the Privacy Impact Assessments on: ▪ Data Protection Impact Assessment completed and reviewed ▪ Reported to Governing Body	May 2018
Data Protection Officers	The Headteacher, Data Manager, Administration Manager and Governing Body have reviewed the steps and actions taken by the school to ensure security of all data in school. As a result the role of the Data Protection Officer will be fulfilled by these individuals. This role fits into the school's structure and governance arrangements as follows: ▪ Reports provided to Full Board each meeting – Named GDPR Governor ▪ Audits completed and reported to the Governing Body and Headteacher	May 2018