The Westminster School

General Data Protection Regulations Policy 2017/2018

Safe Happy and Learning Together

Building foundations and providing opportunities to create confident, aspirational and independent members of our community.

Approved by Governing Body on:	08/06/18
Signed by Chair of Governors:	Ken Ho
Head Teacher:	C A Hill BEd NPQH
Lead Personnel:	J Clarke
Date of Review:	08/06/19

1. Aims

The Westminster 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 and has been out into place to ensure all staff and Governors in the school have an understanding of the scope of the regulation, how it affects them, and the working practices that must be employed on a day to day basis in order to safeguard the personal information of individuals, which we have and use within the school.

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.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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 It may also include factors specific to the individual's physical, physiological, academic, 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. Such individuals must ensure that they are familiar with the contents and behaviours identified within this policy, and should ensure they refer to this policy when carrying out their duties. 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) role is provided by SIPS Education Ltd as a service level agreement.

The DPO is responsible for informing and advising the school and its employees about their obligations to comply with the GDPR and other data protection laws.

The DPO will monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.

The DPO will be the first point of contact for the ICO and will have a direct route of communication with the Head Teacher and the Data Protection Lead (DPL) at the school, providing regular updates on the service and supporting the DPL to complete their role effectively.

Our DPO is Laura Hadley and is contactable via The Westminster School, Curral Road, Rowley Regis, B65 9AN.

5.3 Data Protection Lead

The Data Protection Lead (DPL) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide a 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.

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

Our DPL is Jessica Clarke and is contactable via The Westminster School, Curral Road, Rowley Regis, B65 9AN.

5.4 Head Teacher

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

5.5 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 DPL 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).

The school will undertake a data audit to identify and document those data sets/records held within the school, which contain personal information, and in each case, document the lawful basis for processing. Without a lawful basis, processing must not take place, and the personal data should not be held by the school.

The data audit will be held by the DPL, and should be considered to be a 'live' document. All staff may be asked periodically to assist in reviewing the data audit to ensure all data sets currently in use within the school have been captured and considered, and a lawful basis for processing identified in each occasion.

The school will endeavour to ensure all Data Subjects are clear about the ways in which the school is processing their personal data. This will include publishing information on the type of personal data being collected, the lawful basis for processing, and types of other organisations who the information is shared with, within a privacy notice.

The Privacy Notice will be made readily available by posting this on the school website and making paper based copies available from the school office. A copy of the privacy notice will also be included in the schools' admissions packs and staff inductions.

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.

Internal records will be maintained to reflect the purposes for which processing will take place. More specifically, this will be included on the data audit record, and will include a record of the purpose, description of the categories of individuals and personal data, the categories of recipients of the data (e.g. 3rd party organisations who the School shares the data with); and retention schedules for the personal data.

Appropriate technical and organisational measures that must be maintained in order to safeguard personal data are identified in this policy in general, and will be further documented within Privacy Impact Assessments, if the processing of personal data is higher risk and could result in a risk to the rights and freedoms of the individual.

The school will periodically review its' data capture forms and processes, to ensure that the information being requested is not excessive, and that the school is not capturing more personal information than is required.

Personal data collected by members of staff should, wherever possible, be limited to the scope of what is laid out in official school data capture forms. Wherever there is any

uncertainty about the level of information being requested from Data Subjects, a referral should be made to the DPO for further guidance.

The school shall take proactive steps to check the accuracy of information held within its systems and to subsequently carry out updates as required, through a variety of measures. These include, but are not limited to:

- Issuing data capture forms on an annual basis to parents/carers to verify the accuracy of personal information held on the SIMS system, including: emergency contact details; correspondence address; medical details of the pupils etc.
- Use of apps such as School Comms to allow parents/carers real-time access to the above data on SIMS.
- Issuing data capture forms on an annual basis to staff to verify the accuracy of the personal information held on SIMS.

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 schools data retention schedule.

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, either by letter, email or fax to the DPL. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPL.

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. Similarly, this may also apply to children with Special Educational Needs. 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 DPL in the first instance who will liaise with the DPO as necessary. If staff receive such a request, they must immediately forward it to the DPL.

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. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

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

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

Any enquiries about the CCTV system should be directed to the Head Teacher.

13. 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.

Uses may include:

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

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.

14. 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 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

15. 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
- 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 letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 ICT and Acceptable Use Policy)
- 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)

16. 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.

17. 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

18. 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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

20. Links with other policies

This data protection policy is linked to our:

- ICT and Acceptable Use Policy
- Freedom of information publication scheme
- Information Security Policy
- CCTV 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 on GDPRis and within the T Drive.
- 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 GDPRis and the T drive.

  The DPO, DPL and Head Teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches
We will take actions 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.

A working example:

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*

Appendix 2: General data protection guidelines for staff

Clear desk and clear screen

- PCs should not be left unlocked when workstations are left unattended. PCs can be locked by pressing the windows key and "L" simultaneously.
- Any paper based documents containing personal information should be secured at the end of the day, and when rooms / offices are left unattended. Where there are any concerns over the availability of secure (lockable) storage, or clarification required over the type of information that needs to be secured, staff should in the first instance speak with the data protection lead who will liaise with the Data Protection Officer if required.
- Positioning of computer screens should be considered carefully to ensure only authorised personnel are able to view sensitive or confidential information. This is of particular importance within areas accessed by members of the public, such as the reception area. Privacy screens will be considered where positioning of screens alone will not address this concern.
- Electronic devices should be secured and/or locked away at the end of each day.

Passwords and protection of hardware

- Passwords for accessing systems must be complex enough to make it extremely difficult for third parties to break them: passwords should be at least 8 characters long, have a mixture of upper case and lower case letters, at least one number and one character.
- Passwords should be changed regularly, and never shared with any other member of staff / shared amongst other users.
- Mobile devices (including phones, tablets and laptops) must be protected to the same high standard. You must activate the built in security PIN and set this to the most secure level (if the device allows, this should always be a secure password as detailed above or fingerprint recognition rather than a 4 digit pin

You are personally responsible for any information accessed or disclosed on these devices so it is imperative that you keep your password safe and secure, and do not share it with anyone else.

Accessing and sharing information

There are many different ways in which School staff can access data.

- It is your responsibility to know if you are simply accessing the data that is stored securely elsewhere, or downloading or saving data to a School device.
- Office 365 and the tools it provides allows employees to not only access their emails but actually open, modify, save and /or send any data that is held.
- It is important that employees understand the difference between accessing data (looking at or reviewing) via a mobile or off-site device and downloading/Saving data (this will save a copy of the information onto the mobile device you are using) to a mobile or off-site device.
- Data should not be downloaded or saved to a mobile or offsite device unless you can justify this action with a clear business case for doing so.
- Once the data is no longer required on the device it must be deleted immediately.

There are times when it will be necessary to share information with others.

Inside the School:

- When sharing information with others within the School, if information is of a confidential, sensitive or personal nature, it must be treated as such. Information should only be shared with the individuals who require it, do not copy people into emails if they do not require access to the information contained within. Delete sensitive, confidential or personal information once it has been used for the purpose it has been collected and is no longer required.

Outside the School:
Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods can be used. If in doubt please check with the Data Protection Lead.

- Secure transmission: Where possible, use recognised secure transmission methods such as WebEx.
- Never send personal data within a normal email. If email is the only method of transmission available, ensure the information is included in a password protected document. The password must be agreed with the email recipient in advance, and via telephone, not in another email. Never include the password in the email to which the password protected document is attached, nor send the password via another email (if the first email is intercepted, then the second could also be).
- Ensure that the request for data is a valid one and that only the required data is provided. Always check why people require the data they ask for – if in doubt check with the Data Protection Lead before sending.
- Make sure that the data is up to date. Check the accuracy of the data to be sent before sending
- School Emails should never be sent to public email addresses (e.g. Hotmail, Gmail etc.) regardless of what they contain, unless this has been clearly identified by the recipient as their business email address.

When sending information (including letters) via post the following must be adhered to:

- Always use window envelopes if the address is pre-populated on the enclosed letter to avoid transcription errors or typed labels to avoid issues in relation to legibility of handwriting.
- Always ensure that envelopes are securely sealed. Use additional methods such as sticky tape, glue or staples if deemed necessary
- Double check that no additional information has been included that is not relevant e.g. something mistakenly attached. Only send relevant data. Check that it is valid and accurate and no additional information i.e. additional sheets are included in error.
- If a request is received from an outside agency such as the Police, this should be referred in the first instance to the Data Protection Lead.

Storage of Data on Portable/External Devices

- The loss of any device that can send, store or retrieve data must be reported to your Data Protection Lead and the Data Protection Officer immediately.

- Devices that are capable of transmitting and receiving data information, such as smartphones, should only be used for the purposes for which they were supplied and must be protected by a strong secure password.
- Anyone who uses portable devices to access or store data is responsible for the information which is transported within. This includes USB flash memory devices ("memory sticks"), laptops, external hard disk drives, mobile phones, tablets. Be aware of devices that can access information, such as emails, that could contain sensitive data.
- Any memory stick/portable device that you use for the transport or storage of personal or sensitive nature must be encrypted to an appropriate standard and approved for use by our Data Protection Lead / IT Support. All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information must not be written down and must never be stored or transported with the device. Please be aware an encrypted memory stick/portable device will ALWAYS ask you for a password before use.
- Any storage devices no longer required which may contain information that is surplus to requirements or any device that is in need of secure disposal should be returned to our IT staff or the Data Protection Lead, in person.
- Media such as CDs or DVDs which contain data and are no longer required must be physically destroyed. If you do not have the means to do this, please pass them to the IT Department/Data Protection Lead for disposal – stating clearly that they contain sensitive information
- All portable devices must be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information must not be written down and must never be stored or transported with the device.

Paper and Manual Filing Systems
Paper based (or any non-electronic) information must be assigned an owner. A risk assessment should identify the appropriate level of protection for the information being stored. Paper and files in the School must be protected by one of the following measures:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

It is important that someone has ownership i.e. takes responsibility for the storing and protecting of such systems.

Security of Equipment and Documents Off-Premises
Information storage equipment, data, software or any documents containing personal, sensitive or confidential data should not be used off-site without authorisation from the Head Teacher.

Information storage equipment includes items such as personal computers, organisers, PDAs, tablets, cameras, mobile phones and external storage devices.

The following security guidelines must be adhered to for all equipment and documents taken offsite, it must:

- not be left unattended in public places.

- not be left unattended in a vehicle unless the property is concealed from view and all doors are locked, windows and the roof closed and fastened, all security devices on the vehicle are put in full and effective operation and all keys/removable ignition devices removed from the vehicle
- not be left open to theft or damage whether in the office, during transit or at home
- where possible, be disguised (e.g. laptops should be carried in less formal bags)
- be returned to the School as soon as is practically possible.
- Where it is necessary to transport sensitive or personal data in this manner, data encryption must be in place, and manufacturer's instructions for protecting the equipment should be observed at all times

Physical Security
Our data must be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. This section is related to building security and the level of care that you are expected to provide when transporting computers or paper files outside of the building.

- Our premises are protected by door locks and access codes. It is important that the codes remain secure as these form part of our physical security procedures and as such help to keep our personal, sensitive and confidential data safe.
- Doors and windows must be locked when unattended and external doors (including fire doors) must be locked when not in use.
- All visitors must sign in and receive a Visitor's Authentication Badge. This is issued by the staff in Reception and applies to all Visitors.
- All Visitors/Attendees should be supervised at all times and are required to wear visible authorised identification, and to record their date/time of entry/departure and person(s) being visited.
- Confidential data or computer systems that contain such data - If such access is requested, it is the employee's responsibility to ensure it is a legitimate request and data protection is not breached. If in doubt, please check with your Data Protection Lead or the Data Protection Officer.

I have read and understood the general data protection guidelines for staff detailed above.

Name:

Role:

Signature:

Date: