DATA POLICY

ABSTRACT

The purpose of these policies are to ensure that the school is committed to compliance with all relevant data protection laws

APPROVED	Chair of Governors / Headteacher
POLICY DATE	Autumn 2021
REVIEW	September 2022

DATA PROTECTION POLICY

1.0 Overview

The purpose of this policy is to ensure that the school is committed to compliance with all relevant data protection laws in respect of personal data and to protecting the "rights and freedoms" of individuals whose information is collected. To that end, the School has developed, implemented, maintains and continuously improves data protection policies and procedures.

2.0 Scope and Applicability

The School is a data controller and a data processor under UK GDPR.
This policy applies to all School staff including temporary staff and contractors. Compliance with data protection legislation is the responsibility of all members of the School who process personal information. Therefore, this procedure applies to all personal data processed by the school.

3.0 General Policy

3.1 Objectives

The School is committed to complying with data protection legislation and good practice including:

- Processing personal information only where this is strictly necessary for legitimate purposes
- Collecting only the minimum personal information required for these purposes and not processing excessive personal information
- Providing clear information to individuals about how their personal information will be used and by whom
- Only processing relevant and adequate personal information
- Processing personal information fairly and lawfully
- Maintaining an inventory of the categories of personal information processed by the School
- Keeping personal information accurate and, where necessary, up to date
- Retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate purposes
- Respecting individuals' rights in relation to their personal information, including their right of subject access
- Keeping all personal information secure
- Only transferring personal information outside the European Union in circumstances where it can be adequately protected
- The application of the various exemptions allowable by data protection legislation

3.2 ICO Registration

- The School has notified the Information Commissioner's Office (ICO) that it is a data controller and that it processes certain information about data subjects. The School has identified all the personal data that it processes and this is contained in the Information Asset Register (IAR)

- A copy of the ICO Registration is retained by the Head Teacher and is available to view on the ICO website
- The ICO registration is renewed annually
- The School's nominated person is responsible, each year, for reviewing the details of registration, in the light of any changes to the School's size or structure

3.3 Introduction to UK GDPR

The Data Protection Act 2018 is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation and supersedes the Data Protection Act 1998.

The purpose of UK GDPR is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and that it is processed lawfully.

The UK regulator is the Information Commissioner's Office (ICO) and provides a Guide to the UK GDPR which is used by the Schools Data Protection Officer to understand the detail of the regulation.

3.4 Data Protection Principles

All processing of personal data must be done in accordance with the following data protection principles of the UK GDPR. The School's policies and procedures are designed to ensure compliance with them.

<u>Personal data must be processed lawfully, fairly and transparently</u>

The UK GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language commonly in the form of a privacy notice.

The specific information that must be provided to the data subject must as a minimum include:

- The contact details of the School
- The contact details of the DPO
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- Who the personal data will be shared with
- The period for which the personal data will be stored
- The existence of the data subject rights
- The categories of personal data concerned
- Is the data transferred out of the EU
- Any further information necessary to guarantee fair processing

<u>Personal data can only be collected for specified, explicit and legitimate purposes</u>

- Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of the School's UK GDPR registration.

Personal data must be adequate, relevant and limited to what is necessary for processing

- The School's nominated contact is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Head Teacher
- The Head Teacher will review data collection methods on a regular basis to ensure that collected data continues to be adequate, relevant and not excessive.
- If data is given or obtained that is excessive or not specifically required by the School's documented procedures, the School's nominated contact is responsible for ensuring that it is securely deleted or destroyed in line with the School's retention schedule.

Personal data must be accurate and kept up to date

- Personal Data that is processed must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.
- The Head Teacher is responsible for ensuring that all staff members are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of individuals to ensure that data held by the School is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.
- Staff/Pupils/Others should notify the School of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained on the School's website. It is the responsibility of the School to ensure that any notification regarding change of circumstances is noted and acted upon within 1 month.
- The Head Teacher is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- The School's nominated contact will review all the personal data maintained by the School on a regular basis, by reference to the IAR, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with School's data retention schedule.
- The School's nominated contact is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, for information about them that the information is inaccurate and/or out-of-date is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

- Where personal data is retained beyond the processing date, it will be held securely in order to protect the identity of the data subject in the event of a data breach.
- Personal data will be retained in line with the School's Records Retention Schedule and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

Personal data must be processed in a manner that ensures its security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Data held by the School is secure, controlled and managed. The School's systems and network are regularly independently tested.

Security controls may be subject to audit and review by independent auditors.

The controller shall be responsible for, and be able to demonstrate compliance with accountability

The UK GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the UK GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs, comply with requirements for prior notifications, or approval from the ICO and appoint a DPO.

3.5 External Data Transfers

Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

3.6 Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long

- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations
- The security measures that are to be taken as regards the data in the overseas location

3.7 Data subjects' rights

Data subjects have the following rights regarding personal data that is recorded about them:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

3.8 Complaints

Data Subjects who wish to complain to the School about how their personal information has been processed may lodge their complaint with the DPO.

If Data Subjects are not satisfied with the outcome of their complaint or the way in which it has been handled, they may also complain directly to the ICO.

3.9 Consent

The School understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

The School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For special category data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and special category data is obtained routinely by the School using standard consent documents e.g. when a new member of staff signs a contract of employment, or during induction for participants on programmes.

Where the School provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

3.10 Security of data

All Staff are responsible for ensuring that any personal data which the School holds and for which they are responsible, is kept securely and is not under any condition disclosed to any third party unless that third party has been specifically authorised by the School to receive that information and has entered into a confidentiality agreement.

Any third parties working with or for the School, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the School without having first entered into an agreement which imposes on the third party obligations no less onerous than those to which the School is committed, and which gives the School the right to audit compliance with the agreement.

All personal data should be accessible only to those who need to use it. The School will form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a locked room with controlled access
- In a locked drawer or filing cabinet
- If computerised, password protected
- Encrypted if stored on mobile/removable devices

Care must be taken to ensure that PC screens and terminals are not visible except to authorised members of staff of the School.

Manual records are not to be left where they can be accessed by unauthorised personnel and may not be removed from School premises without explicit authorisation.

Personal data will only be deleted or disposed of in line with the School's Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Storage drives of redundant PCs and mobile devices are to be removed and immediately securely destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site and appropriate security controls implemented.

Security controls may include:

- Data encryption
- Password or PIN protected data
- Secure storage device
- Secure remote access to the data
- Not working in an environment that is not secure or safe such as an internet cafe
- Not keeping laptops or paper records overnight in a vehicle

3.11 Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by the School in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the School, and information obtained from third parties about that person. SARs are dealt with as described in the SAR Procedure.

Disclosure of data

The School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the School's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO. The regulations allow for some exemptions. These too should be discussed with the DPO.

3.12 Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left the School, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. The School's Retention Policy will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

3.13 Security Incidents

The School is required to have internal breach reporting procedures in place as well as external breach reporting procedures. These are detailed in the Schools Security Incident Procedures.

All security incidents are recorded by the school and all staff have been trained to recognise both a security incident and a personal data breach.

The School notifies the DPO of all incidents as soon as practical after the incident has been discovered.

When a personal data breach has occurred, the School in conjunction with the DPO will establish the likelihood and severity of the resulting risk to individual's rights and freedoms. If it is likely that there will be a risk the ICO must be notified. The DPO will report serious data breaches within 72 hours of the incident to the ICO.

Recital 85 of the UK GDPR explains that…"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to

reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Any serious breach of data protection legislation will be dealt with under the School's disciplinary policy and may also be a criminal offence, in which case the matter will be reported to the Information Commissioner's Office (ICO) or Police.

4.0 Roles and Responsibilities

- The Head Teacher and all those throughout the School who are responsible for developing and encouraging good information handling practices.
- The Data Protection Officer (DPO), a role specified in the UK GDPR, is accountable for ensuring that compliance with data protection legislation and good practice can be demonstrated.

This accountability includes:

1. Development and implementation of the UK GDPR as required by this policy; and
2. Security and risk management in relation to compliance with the policy.

- The School's nominated person has been appointed to take responsibility for the School's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the School complies with the UK GDPR, as do staff in respect of data processing that takes place within their area of responsibility.
- The School's nominated person has specific responsibilities in respect of procedures such as the Subject Access Request (SAR) Procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance before contacting the Head Teacher.
- The School`s nominated person will be the conduit between the School and the DPO for security incident reporting.
- The School will ensure appropriate data protection training is provided for all staff.
- Staff are responsible for ensuring that any personal data supplied by them, and that is about them, to the School is accurate and up-to-date.

DATA RETENTION POLICY

1.0 Overview

The General Data Protection Regulation (UK GDPR) states that personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Section 46 of the Freedom of Information Act 2000 requires schools, as public authorities, to follow a Code of Practice on managing their records. Under section 7 of the Code of Practice on the Management of Records, it states that "Authorities should have in place a records management policy".
req

The School recognises and understands that the efficient management of its data and records is necessary to support its core school functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the School.

This policy and related documents meet the standards and expectations set out by contractual and legal uirements and have been developed to meet the best practices of school records management, with the direct aim of ensuring a robust and structured approach to document control and systems.

2.0 Scope and Applicability

The School uses numerous systems and computers as well as paper based records, all of which are within the scope of this procedure. Records are defined as all those documents that are carried out by the school and which are thereafter retained for a certain period to provide evidence of transactions and activities. Records may be created, received or maintained in hard copy or electronic format e.g paper documents, scanned documents, e-mails, spreadsheets, Word documents, presentations etc.

This policy applies to all records created, received or maintained by all School employees including permanent, temporary staff, contractors, consultants or third parties acting on behalf of the School.

3.0 General Policy

3.1 Retention schedule

We follow the IRMS Toolkit for retention periods. This informs our retention periods for various levels of personal data.

3.2 Information Asset Register

The School holds and maintains an Information Asset Register (IAR). This records:

- The information retained
- The legal basis for holding the data
- The type of information i.e. personal information, special category data
- Where the information is held
- The "owners" of the data
- Who the data is shared with
- The retention period

The IAR allows the school to manage the information that is held which includes information created, held, received and in use. This document enables the School to identify the personal information it creates and stores to facilitate correct management under the Data Protection Act (DPA)2018, the General Data Protection Regulation(UK GDPR) and the Freedom of Information Act 2000.

3.3 Guidelines and Procedures
The School manages records efficiently and systematically, in a manner consistent with the UK GDPR requirements.

Records will be created, maintained and retained in order to provide information about, and evidence of the School's transactions, customers, employment and activities. The retention schedule will govern the period that records will be retained.

It is our intention to ensure that all records and the information contained therein is:

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (with additional security permissions for select staff where applicable to the document content)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Monitored** – staff, School and system compliance with this Data Retention Procedure is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

3.4 Destruction and Disposal of Records and Data
All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with Data Protection laws and the duty of confidentiality owed to data subjects.

The School is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that is done so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the UK GDPR and that staff are trained and advised accordingly on the procedures and controls in place.

3.5 Right to Erasure
In specific circumstances, data subjects have the right to request that their personal data is erased, however the School recognises that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies: -

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed

- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and the School received a request to erase data, there must be a check to ensure that no other legal obligation or legitimate interest applies. If the data subject has the right to have their data erased, this is carried out by the School's nominated person in conjunction with the person responsible for IT to ensure that all data relating to that individual has been erased.

These measures enable the School to comply with a data subjects' right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst standard procedures remove data that is no longer necessary, the School follows a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

3.6 School Archives

The School archive is maintained as a resource to help inspire and equip current staff and pupils to understand and appreciate issues of identity, belonging and shared heritage to prompt memories of school-life among many generations and to serve as a research resource for all interested in the School and the community it serves.

4.0 Roles and Responsibilities

The governing body has the statutory responsibility to maintain the School records and record keeping systems although the head takes day to day responsibility.

The Schools UK GDPR lead person will give guidance on good records management practice and will refer to the Schools Data Protection Officer (DPO) when required.

CCTV POLICY

1.0 Overview

The purpose of this policy is to ensure that the school complies with the regulatory requirements, in particular, the Data Protection Act 2018 (DPA) when using a closed-circuit television (CCTV) system at the school.

The system comprises a number of cameras located around the school site. Cameras are situated both internally and externally.

2.0 Scope and Applicability

This policy applies to the entire CCTV system which includes cameras situated internally and externally. It also includes the monitoring of the system.

3.0 General Policy
The school will treat the system and all information, documents and recordings obtained and used, as data which is protected by the DPA.
The system installed is compliant with the DPA, Human Rights Act and Regulatory Investigation Powers Act.

Cameras will be used to monitor activities within the school and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the school and its staff, students and visitors.

3.1 Storage and retention of CCTV images
Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their value as evidence and to protect the rights of the people whose images have been recorded. All retained data will be stored securely, using on site systems. Data may also be held in online storage platforms for backup purposes.

The data is stored on a rolling 30 day basis. Following this retention period, the data is securely destroyed.

Regular audits are conducted to ensure that all cameras are operating correctly and that footage is clear.

3.2 Access to CCTV images
Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available. If a staff member without authorisation is found to be accessing the equipment or footage, this may lead to disciplinary action being taken.

3.3 Subject access requests (SAR)
Individuals have the right to request access to CCTV footage relating to themselves under the DPA.

All such requests should be directed to rachel.roberts@grange.newham.sch.uk and processed in line with the subject access request procedure. Individuals submitting requests for access will be asked to provide sufficient information to enable the relevant footage to be identified. For example, date, time and location.

In line with data protection regulations, the school will respond to requests within a month of receipt unless there are extenuating circumstances in which case a further two months extension may be required.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

The following categories of staff have access to CCTV footage:
Senior Leaders
Office Administrative staff

3.4 Access to and disclosure of images to third parties
There will be no disclosure of recorded data to third parties other than to authorised personnel such as the police and service providers to the school where they would reasonably require access to the data (e.g. investigators).
Requests from police and other professional services should be made to the Head Teacher.

CCTV data may be used within the school's disciplinary and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Information from CCTV will not be used for any commercial purpose. Information transferred to DVD (or other appropriate media) will only be used for the investigation of a specific crime or incident. Release to the media will only be permitted with the written authority of the police if this was required as part of a police investigation.

3.5 Signage
The school will erect signs to ensure individuals are aware that they are in an area where camera surveillance is in operation.

The signs will be clear, visible, readable and will contain the contact details for the school as well as the purpose for using a surveillance system.

3.6 Complaints
Complaints and enquiries regarding the operation of CCTV on the school site should be directed to the Head Teacher in the first instance. Any such complaints will be dealt with under the terms of the school's complaints policy.

3.7 Roles and Responsibilities
There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held, recorded and used and to whom it may be disclosed.

As Data Controller, the school is both legally responsible and accountable for the control of onsite CCTV. As such the school will allocate an individual for this task.

Therefore the Head will take ultimate responsibility for the CCTV. However, the Site Supervisor has day to day responsibility for the CCTV system.

4.0 References

Further information on CCTV and its use is available as follows:

- In the picture: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- www.ico.org.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018
- The Protection of Freedoms Act 2012

SECURITY INCIDENT PROCEDURE

1.0 Overview

The School maintains a robust and structured program for data compliance and monitoring. However, not all risks can be completely mitigated and security incidents may occur from time to time despite best endeavours.

The protection and security of the data that is processed by the School, including personal information, is of paramount importance to the School. Data specific controls and protocols have been developed for any breaches involving confidential information and personal data.

The purpose of this document is to describe the School's policy and procedure for data security incidents including the recording and reporting of personal data breaches.

2.0 Scope and Applicability

This procedure applies to all security incidents that occur within the school environment. This extends to remote working. Security incidents which occur in any of the Schools Processors are also included within this procedure.

All staff have a responsibility to identify and record any security incidents relating to the potential loss of School data. Therefore, this procedure is applicable to all staff involved with the running of the school including employees, contractors and agency staff.

The School's definition of a security incident for the purposes of this procedure is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to data.

3.0 General Procedure

The School captures all security incidents as it allows the School to understand areas of weakness and highlights changes that should be made to policies and procedures to ensure effectiveness.

Any security incidents that are found to include personal data must be treated in accordance with this procedure and the UK GDPR.

3.1 Identification of Incidents

The School's definition of a security incident for the purposes of this policy is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to data.

The recording of security incidents shall take place irrespective of how the incident occurred and who was responsible.

Prompt action may be necessary to reduce the potential impact of an incident, so there may be occasions when an incident is resolved before it is recorded. If this occurs, a breach incident form should be completed as soon as possible after the event.

Where a processor suffers a data breach, the processor will notify the School as soon without undue delay. The School is responsible for notifying the DPO and following all notification procedures in the same way that the School will deal with internal incidents.

3.2 Incident Reporting

The School will captures all security incidents as it allows the School to understand areas of weakness and highlights changes that should be made to policies and procedures to ensure effectiveness.

Any security incidents that are found to include personal data must be treated in accordance with this procedure and the data protection legislation.

Staff have been trained to identify a security incident and the procedure for reporting it.

As soon as a security incident has been identified, it must be reported immediately to the DPO so that breach procedures can be initiated and followed without undue delay.
The School is committed to complying with legislation without apportionment of blame.

It is important that every incident, however minor, is recorded and follows this procedure to ensure that the probability of reoccurrence is avoided or reduced, and the impact of future incidents is minimised.

In the case of a security incident, a member of staff will complete a Breach Reporting Form which is then sent to the DPO. All staff have the link to the online reporting form.

3.3 Incident Investigation

Security Incidents can originate from human errors or system errors. The DPO will analyse recorded security incidents in order to ascertain whether or not personal data has been compromised. Each incident will be prioritised according to severity, which will be based upon the actual or potential impact of the incident upon and will be categorised as:

- Critical (C)
- High (H)
- Medium (M)
- Low (L)

For example, in the case of a 'Low' severity, 'no action' may be an acceptable option. In the case of a 'Critical' severity, the DPO will ascertain whether or not personal data has been compromised.

If personal data has not been compromised, the security incident will be referred to the Head Teacher for further consideration.

If personal data is found to have been compromised, the DPO will make recommendations to the School as to which immediate actions should be taken to mitigate the impact of the incident. Recommendations will also be made to prevent any future occurrence of the same root cause.

3.4 Personal Data Breach Notification
The DPO will review each personal data breach and will decide if notification to the Information Commissioner's Office (ICO) is required.

The ICO is to be notified of any personal data breach where it is likely to result in a risk to the rights and freedoms of individuals.

Affected Data Subjects are to be notified without undue delay of any personal data breach where it is also likely to result in a risk to the rights and freedoms of individuals. The DPO will provide guidance to the school as to the appropriate course of action.

3.5 Notification to the ICO
Where applicable, the DPO will notify the ICO of the personal data breach no later than 72 hours after the School becomes aware of the incident and are kept notified throughout any breach investigation. The ICO will be provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

The following information will be included in the notification to the ICO:

- A description of the nature of the personal data breach
- 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 taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects

The DPO will notify the ICO via telephone or the online reporting system.
Where the School does not have full information regarding the personal data breach, a partial report should be submitted to the ICO with subsequent reports to follow as information becomes available.

The ICO will provide the DPO with an acknowledgement of the notification. In due course the ICO will either request more information from the DPO or will advise the DPO of the outcome following their investigation. The DPO will keep the School abreast of all developments.

3.6 Data Subject Notification
Where applicable, the DPO will ask the School to notify data subjects of the personal data breach without undue delay. Data subjects will be provided with the following:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

A full report will be provided in a written, clear and legible format.

3.7 Record Keeping
All records and notes taken during the identification, recording, investigation and notification of the security incident are recorded and authorised by the DPO and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed regularly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

4.0 Roles and Responsibilities
As Data Controller, the school is responsible for complying with all security incidents.
Each member of staff is responsible for reporting security incidents that they are aware of.
The School's Data Protection lead person is responsible for notifying the DPO of any security incidents as and when they occur.

SUBJECT ACCESS REQUEST PROCEDURE

1.0 Overview
Data subjects have the right to obtain confirmation that their data is being processed, access to their personal data and the right to be informed of processing via a privacy notice. The right of individuals to access their personal information can be fulfilled via a subject access request (SAR).

2.0 Scope and Applicability
This procedure applies to all personal data processed by the school and to all staff who deal with SARs.

Paper and electronic records are to be considered for inclusion within a SAR response.

The request may be received from a parent, a pupil or a third party such as a solicitor.

3.0 General Policy
Two reasons for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

The school must provide a copy of the information free of charge unless the request is manifestly unfounded or excessive, particularly if it is repetitive. The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt. The day the request is received counts as day 1 and the response must be supplied by the corresponding date in the next month. Should this be a weekend or public holiday, the following working day will be the deadline. Where there is no corresponding day in the month, the last working day in the month will be the day required in order to comply with the rules.

The School will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the individual must be informed within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the School can:

- Charge a reasonable fee taking into account the administrative costs of providing the information
- Refuse to respond

When a request is refused, the School must explain the reason to the individual, informing them of their right to complain to the Information Commissioner's Officer (ICO) and to a judicial remedy without undue delay and at the latest within one month.

3.1 Request for Personal Data

SARs may be received via various methods including email, letter, telephone or in person. Any request from an individual for personal information will be treated as a SAR. Whilst the School cannot insist upon the completion of a SAR form (See Appendix 1 for an example SAR form), data subjects should be directed to complete and submit a form as this will aid the fulfilment of the request and narrow the requirements which will reduce the workload for the school and provide more meaningful information to the data subject.

3.2 Verification of Identity

In most circumstances, it will be necessary to verify the identity of the requestor. An exception would be where the requestor attends the school in person asking for their or their child's personal data and the requestor is known to the school.

Where there is a need to verify the identity of an individual, the requester will be asked to verify their identity by providing acceptable documentation.

One item from list A and one item from list B is required.

List A	List B
Photographic proof of identification	Proof of address
Passport	Bank Statement
Photographic Driving License	Utility Bill

The requester should present the identification documents in person to the school promptly. The documents will be verified and the request will move to the fulfilment stage.

Under no circumstances should information be disclosed to anybody prior to their identity being verified.

3.3 Fulfilment of Request

The School's nominated person will review the SAR in conjunction with the Information Asset Register to ascertain whether or not personal data is being processed by the school. The School's nominated person will then liaise with the relevant information asset owners in order to collate the required information.

Original documents are not required to be provided. A copy can be provided or multiple documents containing personal information can be transposed into a single document. Any personal information relating to data subjects not named in the SAR, must be redacted unless consent to disclose the individuals name has been received.

If the request is made electronically, the school should provide the information in a commonly used electronic format. Personal information can also be provided in paper formats.

There is no exemption for requests that relate to large amounts of data, but the School may be able to consider whether the request is manifestly unfounded or excessive. Additional time is permitted where cases are particularly complex with a maximum extended period of two months. Where this is likely to apply, the school should notify the requester of the delay and the reason for it.

3.3.1 Exemptions

There are certain exemptions which means that the school can refuse to comply with a subject access request (wholly or partly). An example of an exemption is the Crime and Taxation exemption which may be used when the data subjects personal data has been provided to police for an investigation.

All cases should be considered on a case by case basis and each one where the school believes an exemption may apply should be referred to the Data Protection Officer (DPO) for guidance.

3.3.2 Sending documentation

Paper documentation will be packaged and sent via Royal mail. Alternatively, the requestor can collect the package from the school.

The School's preferred method of sending the documentation is via electronic means. This will usually be achieved by scanning the electronic redacted documents into a file. The file will then be sent electronically using a secure system such as USO FX or Egress. Any other specific requests should be referred to the DPO.

3.4 Recording of Request

In order to determine if a request can be deemed to be repetitive, records of SARs will be kept. This record in itself will be subject to any future SARs and should be retained in line with the School retention schedule.

The school will maintain a log of all SARs with a chronology of events for each SAR received by the school. This log may also be useful should the requestor lodge a complaint with the regulator as the timescales and the method of response can be easily supplied.

4.0 Roles and Responsibilities

As Data Controller, the school is responsible for complying with subject access requests and ensuring that staff are aware of their data protection obligations.

CONSENT PROCEDURE

1.0 Overview

All personal data under the General Data Protection Regulation (UK GDPR) must be lawfully processed. Consent is a legal basis which can be used to ensure that personal data is lawfully processed. However, the use of consent is onerous and wherever possible an alternative legal basis should be sought. The School may be required to seek consent from Data Subjects which include staff, parents/guardians and pupils.

Consent provides individuals with real choice and control over use of personal data. Genuine consent puts individuals in charge, builds customer trust and engagement, and enhances reputation.

The UK GDPR provides five other ways of processing data that may be more appropriate than consent particularly in the education sector. It is unlikely that consent will be used for curricular activities as sufficient statutory powers exist which provide a more suitable legal basis.

Data subjects have the specific right to withdraw consent. The school is required to inform data subjects about their right to withdraw, and offer them easy ways to withdraw consent at any time.

2.0 Scope and Applicability

This procedure applies to all personal data processed by the school and where the school is using consent as a lawful basis for processing personal data.

3.0 General Policy

The School shall be able to demonstrate that the data subject has given explicit consent to the processing of his or her personal data.
Wherever consent is requested, clear, plain language that is easy to understand will be used.
Data subjects will be required to positively opt in (pre ticked 'opt out' boxes will not be used).

3.1 Requesting Consent

Consent must be freely given and the data subject must have a genuine choice as to whether or not they wish to provide their personal data. For example a staff noticeboard with photographs is not essential for the running of the school and therefore consent is likely to be required.
When relying on consent, the School ensures that the pupil understands what they are consenting to. The School will not exploit any imbalance in power in the relationship between the School and the pupil.
Extra-Curricular activities which require the use of personal data (such as school photographs, after school Clubs) are likely to require written consent as there is unlikely to be another legal basis which applies.

The UK GDPR does not prescribe the age at which a pupil is considered to be a child with the exception of online services which are 13 years of age. The School shall be able to demonstrate that, where the data subject has given explicit consent to the processing of his or her personal data for online services, and the processing relates to a pupil under 13 years old, additional

consent has been received by the person who is the holder of parental responsibility over the pupil.

The School shall be able to demonstrate that reasonable efforts have been made to establish the authenticity of the parental responsibility.
The School will make available Privacy Notices to Parents/pupils which will reflect that consent as a legal basis is being used.

3.2 Recording Consent
The school will be responsible for keeping records of how and when consent was obtained. Records of consent and privacy notices which were provided should be retained for the duration of the processing activity. See Appendix 1 for an example pupil consent form.

3.3 Managing Consent
The school will regularly review records of consent to ensure that they remain relevant and up-to-date. If the consent held by the school is no longer relevant, re consent will be sought at the appropriate time.

3.4 Withdrawal of Consent
The school will ensure that individuals are able to withdraw their consent at any time and ensure that requests are promptly processed. Data subjects who choose to withdraw consent will not be penalised in any way.

4.0 Roles and Responsibilities
The School (as a data controller) is responsible for requesting, recording and managing consent which includes processing withdrawal of consent from data subjects.

COMPLIANCE

All staff are expected to comply with the School's policies to the highest standards. If any School employee is found to have breached this policy, they may be subject to the School disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

DEFINITIONS

DPA - Data Protection Act

IAR - Information Asset Register

SAR - Subject Access Request

UK GDPR - The General Data Protection regulation

ICO-Information Commissioner's Office

Territorial scope – the UK GDPR applies to all controllers that are established in the EU who process the personal data of data subjects. It applies to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The School is a data controller.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – The UK GDPR does not define the age at which a person is considered to be a child. The processing of personal data of a child under 13 years of age in relation to online services is only lawful if parental or guardian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis