Mayfield	Policy Name: Data Protection Policy Owner: Bursar Date : Reviewed Sept 2023 Date Next Review Due: Sept 2024 This policy will be revised as regulations or review demands.

Everyone has rights with regard to the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious case reviews where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe.

Those who are involved in the processing of personal data are obliged to comply with this policy when doing so. Any breach of this policy may result in disciplinary action.

This policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

This Policy also makes reference to the principles contained in the Document Retention Procedure (contained in Annex A) which should be read in conjunction with this document. The general principle is that all information held by the School must be legally justifiable and there must be a relevance and purpose in retaining data.

- All information held by the School needs to be justifiable by reference to its purpose;
- The School is transparent and accountable as to what it holds and understand why;
- The School is prepared to respond quickly to subject access requests;
- The School is able to amend, delete or transfer data promptly upon receiving a justified request;
- Any personal data that is collected should be auditable as far as possible; and
- Personal data must be held securely and accessed only by those with reason to view it.

Purpose of the Policy

The School is required to process relevant personal data regarding workers, pupils, parents, governors, donors, contractors, ex-pupils and visitors as part of its operation and shall take all reasonable steps to do so in accordance with this Policy and in accordance with the Data Protection Act 2018 and the UK-GDPR Regulations. This Policy sets out how data will be controlled, maintained, archived and destroyed. This Policy takes into account

- Statutory duties and government guidance relating to schools including Safeguarding;
- Disclosure requirements for potential future litigation;
- Contractual obligations;
- The law of confidentiality and privacy; and

- Data Protection Legislation / UK-GDPR

This Policy sets out both the minimum and maximum retention periods for personal data but also what to keep and who should be able to access it.

Data Protection Supervisor

The School has appointed the Bursar as the Data Protection Supervisor who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 2018 which should be read in conjunction with the UK-GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Supervisor.

Definitions

For the purposes of this Policy the word 'record' means any document or item of data which contains evidence or information relating to the School, its staff, pupils and parents. It could also refer to visitors, contractors and governors. Some of this material but not all, will contain personal data of individuals as defined in the legislation.

Personal data means any information that can directly or indirectly identify an individual in this context. UK -GDPR also defines 'sensitive personal data as special categories of personal data which is more sensitive and therefore needs more protection. This includes information about an individual's:

- Race;
- Ethnic origin
- Politics
- Religion
- Trade Union membership;
- Genetics;
- Biometrics (where used for ID purposes)
- Health;
- Sex life; or
- Sexual orientation

This Policy applies to both electronic records and paper documents or records. The format of the record is less important that its content or the purpose for keeping it.

The Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the Data Protection Act 2018. These provide that personal data must be: -

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- Accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Processing of Personal Data

The School's policy is to process personal data in accordance with the applicable data protection laws as set out above. All staff have a personal responsibility for the practical application of this policy.

Staff should generally not process personal data unless:

- The processing is necessary to perform the School's legal obligations or to comply with a contract, or
- The processing is otherwise in the School's legitimate interests and does not unduly prejudice the individual's privacy; or.
- The data subject has explicitly consented to the processing of their personal data; or
- it is necessary to protect the life of the Data Subject or other person

When gathering personal data or establishing new data protection activities, staff should ensure that individuals whose data is being processed receive appropriate privacy notices to inform them how the data will be used. In any case of uncertainty as to whether a notification should be given, staff should contact the Data Protection Supervisor.

Sensitive Personal Data

The School may, from time to time, be required to process sensitive personal data regarding a worker or a student. This type of data could create a more significant risk to an individual's fundamental rights and freedoms. Where there need to process data of this nature this must be discussed and agreed with the Data Protection Supervisor to ensure that the appropriate measures are taken to reduce the risk to the individual.

Where sensitive personal data is processed by the School and explicit consent is required e.g. access to an individual's medical records this consent must be:

- freely given;
- require a positive action to opt in; consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand and be user-friendly
- confirmed in words
- Able to be withdrawn

The School recognises that due to the nature of the relationship between itself and its employees consent can rarely be freely given and so this is only used in exceptionally limited circumstances e.g. where the School requests a medical report from an individual's GP.

Processing of Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar.

Accuracy, adequacy, relevance and proportionality

Staff should make sure data processed by them is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless there is a legal basis (as defined in the regulations) for doing so. Where there is an entirely new purpose than a new Privacy Notice may need to be issued to the relevant individuals to make them aware of these changes.

Individuals have the right to expect the School to correct personal data relating to them which they consider to be inaccurate or incomplete. This is called the Right of Rectification. If a member of staff receives such a request they must forward this to the Data Protection Supervisor where the request should be acknowledged. If the personal data is to be corrected this must take place within one month of receipt of the request and confirmed to the individual. This timeframe can be extended to two months where the request is complex. Where the School does not agree to action a request this must be explained to the individual stating the reasons why and informing them of their right to complain to the supervisory authority and to a judicial remedy.

Staff have a responsibility to ensure that personal data held by the School relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform their line manager, the HR Manager or the Finance Manager as appropriate so the School's records can be updated.

Right to Erasure

Also known as the 'right to be forgotten' this right enables an individual to request the deletion of removal of personal data where there is no completing reason for its continued processing. This is not an absolute right and only applies in specific circumstances such as where the data collected is no longer necessary for the purpose for which it was collected. The School can refuse to comply with such a request where there is an overriding legitimate interest for continuing with the processing.

Right to Object

Individuals have the right to object to processing based on legitimate interests; there are additional legal basis under which an individual can object but this is the one that is relevant to the School. Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

For an individual to object they must have an objection on "grounds relating to his or her particular situation". Where such a request is received the School must stop processing unless:

- It can demonstrate a compelling legitimate grounds for processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Individuals are made aware of their right to object at the point of first communication and as part of the School's privacy notice.

Right of Access

Individuals have the right to access their personal data and to be aware of and verify the lawfulness of processing. Individuals have the right to obtain confirmation that their data is being processed, to access that data and this includes "other supplementary information".

The School will provide this information free of charge but reserves the right to charge a 'reasonable fee' where a request is manifestly unfounded or excessive. This fee will be based on the administrative costs of providing the information.

The School will comply within one month of receipt of an access request but this may be extended where a request is particularly complex or numerous. Where this is the case the individual making the request will be informed of this in writing within the original one month deadline and provided with an explanation as to why this extension is necessary.

Where such a request is made the School will use 'reasonable means' to verify the identity of the individual making that request usually be requesting that ID documentation such as passport or driving licence is provided with that request. Where the request is received electronically the School will respond electronically using a commonly used electronic format.

Where the School possess a large quantity of information about an individual they will ask the individual to specify what information is required. This may take the form of a specific date period or relate to a specific matter.

Other individual rights

Under the regulations individuals also have the right to be informed about the personal data that the School is processing. The School provides all individuals with Privacy Notices which set out in a transparent way fair processing information.

The Privacy Notice will contain:

- Identity and contact details of the data controller and the data protection supervisor
- The purpose of the processing and the lawful basis for it
- The legitimate interests of the controller or third party
- Categories of personal data
- Any recipient or categories of recipients of that personal data
- Details of transfers to countries outside of the UK and safeguards in place
- Retention periods
- The data subject's rights
- The right to withdraw consent
- The right to lodge a complaint with a supervisory authority

- The sources that the personal data originates from and whether it came from publicly accessible sources
- Whether the provisions of personal data is part of a statutory or contractual obligation and possible consequences of failing to provide the personal data
- The existence of automated decisions making (where applicable)

Individuals also have the right to restrict or block processing in certain limited circumstances. Where processing has been restricted the School can store personal data but not further process it.

Paper Records

By their very nature paper records can be damaged by damp or poor storage conditions and should therefore kept in a dry and cool environment with reasonable ventilation away from direct sunlight. They should not be stored with metal, rubber or plastic which can deteriorate and damage the paper.

Records will be kept securely in an appropriate locked facility where access is strictly limited to those who have a legitimate and genuine need to do so. Keys to archiving rooms or cupboards will be controlled and only those who had a legitimate need, as part of their role within the School, to access the data when it was current will be able to gain admittance. For example staff personal files will only be accessible to the HR Manager and members of SMT.

The legislation applies to manual filing systems or paper records where personal data is readily accessible and searchable in the same way as an electronic database may be. Where there is any doubt as to whether a manual filing system is covered by the legislation the School will assume that it is and ensure that it is treated in line with the Policy. Any paper records that are print-outs from electronic files have already been processed by the School and therefore automatically fall under the Policy.

Data Management

All staff receive training in basic data protection and therefore will be aware of issues such as security, recognising and handling sensitive personal data and Safeguarding. Staff who are given specific responsibility for the management of records will ensure the following:

- That records whether electronic or hard copy are stored securely so that access if only available to authorised persons.
- That records containing personal information whether relating to pupils, parents, staff, visitors or contractors are not taken home or in respect of digital data carried or kept on portable devices unless necessary in which case it would be subject to a risk assessment and in line with the current ICT Policy. Records that contain sensitive personal data will not be taken off site unless it is with the explicit consent of the data protection supervisor and relevant member of SMT.
- Only relevant key personnel who have received appropriate training are able to delete or erase data and then only in line with this Policy. The ICT Department will ensure that access to delete data is strictly controlled.
- Regular back-ups of digital personal data will be taken in line with the current ICT Policy.
- Where external storage providers are used – whether electronic (in any form but particularly “cloud based” storage) or physical – the arrangements will be supported by robust contractual arrangements which detail the providers’ data security provision. All provisions must be in line with the School’s ICT Policy.
- Annual reviews will be held on records to ensure that all information being kept it still relevant and in the case of personal data still necessary for the purposes for which it is being held. If it is deemed to still be necessary then it must be reviewed to ensure that it is accurate and up to date.
- Only staff who have received the relevant training and who have the appropriate level of authority will be able to destroy or permanently delete records from School databases or centrally held

records. Regular reviews of these systems will be regularly taken place and if required records will be archived.

- Staff members who have created their own records must ensure that they destroy any paper based records which contain personal information. Documents must be securely disposed of which means that it must not be in a condition where they can still be read or reconstructed. Records that contain personal information must not be placed in recycling bins or thrown in general waste bins. Paper records should be shredded using a cross cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard copy images, AV recordings and hard disks should be dismantled and destroyed.
- Where third party disposal experts are used they will be supervised by an appropriate member of staff but will under contractual obligations to process and dispose of the information in a manner appropriate.

Retention of Records

Under the terms of the Data Protection Act 2018 and the UK-GDPR regulations personal data can only be kept for as long as is necessary for the specific lawful purpose that it was acquired for. However the School must ensure that it keeps records for a number of different reasons but primarily as a defence against litigation. Generally speaking the School will be in a better place to deal with any claims that may arise if it has adequate records in place to support its position or a decision that has been made. For further information on the retention of records please see the Retention of Records Policy.

Appendix A – Document Retention Procedure

The School collects, stores and processes personal data about Governors, Staff, pupils, ex-pupils their parents, suppliers and other third parties as part of its normal day to day activities

The School will seek to balance the benefits of keeping details and complete records for the purposes of good practice, archives or general reference with practical considerations of storage, space and accessibility. In addition to this there are also legal considerations in respect to the retention of records and documents including:

- Statutory duties and government guidance relating to schools, including for safeguarding;
- Disclosure requirements for potential future litigation;
- Contractual obligations
- The law of confidentiality and privacy
- The Data Protection Act (DPA)

These inform not only minimum and maximum retention periods but also what to keep and who should be able to access it.

Meaning of 'Record'

For the purpose of this Policy 'record' means any document or item of data which contains evidence or information relating to the School, its staff or pupils. Some of this material, but not all of it, will contain personal data of individuals as defined in the DPA.

Whilst many of these records will be created, received and stored electronically other records will be original paper documents. The format of the record is less important that its contents and the purpose for keeping it.

Digital Records

Digital records can be lost or misappropriated in huge quantities very quickly. Access to data will always be password protected as a minimum and access to data that is considered to be sensitive will be controlled. Only those individuals who require access for their specific role within the School will be able to view or otherwise process this data.

Emails, whether retained electronically or printed out as part of a paper file, are also records and may be particularly important as either disclosable documents in any litigation or as representing personal data of the sender (or subject) for data protection purposes. Particular care should be taken when setting up automatic rules around the deletion of emails and users should be mindful that archived records may still remain on servers or in cloud storage facilities.

Paper Records

Paper records are easily damaged via damp or poor storage conditions; they will be kept in cool, dry, ventilated areas away from direct sunlight and not stored with metal, rubber or plastic which may damage the paper as it deteriorates. The School has designated archive facilities for paper records and staff should speak to the Bursar in the first instance if they need to retain paper records other than those already held by the School. All paper records held within the School are only to be accessible by those who role within the School would require them to need access.

Archiving and the destruction or erasure of Records

All staff receive training in relation to Data Protection via E-Learning and staff who have specific responsibility for the management of records have training to ensure that they maintain the following minimum standards:

- That records – whether electronic or hard copy – are stored securely with access only available to authorised persons and the records are available when required in a searchable condition;
- That important records, and large or sensitive personal databases are not taken home or in respect of digital data – carried or kept on portable devices unless absolutely necessary. Where this is necessary or those databases can be accessed remotely it is done so in line with the School's Acceptable Use of ICT Policy;
- Back-up and migration is carried out by the School's IT Department as a general rule but where this is not possible or practicable it is done in consultation with them and in line with their Policies;
- Arrangements with external storage providers are supported by robust contractual arrangements providing for security and access;
- Reviews are carried out regularly to ensure that all data being kept is still relevant, necessary for the purpose for which it is held (and if so is accurate and up to date); and
- All destruction or permanent erasure of records, if undertaken by a third party, is carried out securely, with no risk of the re-use or disclosure or re-construction of any records or information contained in them.

Note

The Independent Inquiry into Child Sexual Abuse (IICSA) has issued retention instructions to a range of institutions, including Schools, requesting the preservation of all records relating to the care of children so that they can remain available for inspection by the Inquiry. Therefore records will be preserved for as long as necessary to fulfil any potential legal duties that may arise out of the Inquiry. The obligation to retain documents will remain through the duration of the Inquiry.

Table of Retention Periods

Type of Record / Document	**Retention Period**
School Specific Records • Registration Documents of School	• Permanent (or until closure of the School)
• Attendance Register	• 6 years from last date of entry, then archive
• Minutes of Governors' meetings	• 6 years from date of meeting
• Annual Curriculum	• From end of year: 3 years
Individual Pupil Records • Admissions: application forms, assessments, records of decisions	• 25 years from date of birth
• Examination Results (external or internal)	• 7 years from pupil leaving the School
• Pupil file including: o Pupil reports o Pupil performance records	• All: 25 years from date of birth (subject to where relevant to safeguarding considerations; any material which may be relevant to potential claims should be kept for the lifetime of that pupil)

○ Pupil medical records • Special educational needs records	• Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
Safeguarding • Policies and procedures • DBS Certificates • Accident / Incident Reporting • Child Protection Files	• Permanently • No longer than 6 months from the decision on recruitment but a record of the check being made is to be kept along with the certificate number • To be kept for as long as any living victim may bring a claim. • If a referral has been made / social care has been involved or child has been subject of a multi-agency plan records are to be kept indefinitely If low level concerns with no multi-agency involvement then treat as pupil file so 25 years from date of birth
Accounting Records • Accounting Records • Tax Returns • VAT Returns • Budget and internal financial reports	• 6 years (except where still necessary for tax returns) from the end of the financial year in which the transaction took place • 6 years • 6 years • 3 years
Contracts and Agreements • Signed or final / concluded agreements (including variations or amendments) • Deeds (or contracts under seal)	• 7 years from completion of contractual obligations or term of agreement, whichever is the later • 13 years from completion of contractual obligation or term of agreement
Intellectual Property Records	

• IP / IT agreements (including software licences and ancillary agreements e.g. maintenance, storage, development etc.	• 7 years from completion of contractual obligation or term of agreement
Employee Records	
• Single Centre Register of employees	• Permanent record of all mandatory checks (but no DBS certificate itself)
• Contracts of employment	• 7 years from the effective end of contract
• Employee appraisals or reviews	• Duration of employment plus 7 years
• Staff Personal File	• 7 years
• Payroll, salary, maternity / paternity / adoption pay records	• 7 years
• Pensions or other benefits records	• 7 years
• Job application and interview records (unsuccessful candidates)	• 6 months unless unsuccessful candidates consents to the retention of record for longer
• Immigration Records	• 7 years
• Health records relating to employees	• 7 years from end of contract of employment
Insurance Records	
• Insurance Policies	• Duration of policy (or as required by policy) plus a period for any run-off arrangements and coverage of insured risks
• Correspondence related to claims / renewals / notifications	• 7 years
Environmental, Health & Data	
• Maintenance logs	• 10 years from date of last entry
• Accidents to children	• 25 years from birth (longer if relevant to safeguarding)
• Accidents at work records (staff)	• 4 years from date of accident but should be reviewed on a case by case basis

• Staff use of hazardous substances	• 7 years from end of date of use but should be reviewed on a case by case basis
• Risk assessments (on the above)	• 7 years from completion of relevant project, incident, event or activity
• Data protection records documenting processing activity and data breaches	• No time limit as long as up to date and relevant

Appendix B – Subject Access Request Procedure

Under the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK-GDPR) all individuals have the right to know what personal data about them is being held and used by organisations. They also have the right to know the purpose for which it is being held, where it came from and who else might receive it. More information about an individual's rights under data protection legislation can be found in the School's Data Protection Policy.

A Subject Access Request (SAR) is a written request made by or on request of an individual under section 7 of the DPA.

This Policy sets out how the School will respond to such a request.

What is a SAR?

A SAR must be made in writing but does not have to mention the DPA or the UK-GDPR. The SAR must make it clear that the requester wishes to access information about themselves (or an individual on whose behalf they are acting) held by the School. It can be made to anyone in the organisation and can be made on-line.

The School can request any information that they require to reasonably be able to confirm the identity or authority of the requester or in order to locate the data sought.

Can a SAR be made on another's behalf?

Provided that the School is satisfied that the third party is acting genuinely on the individual's behalf e.g. a family member or perhaps a solicitor, then the SAR should be actioned as if it is from the individual themselves. Students have exactly the same rights as adults and can therefore make a SAR and indeed strictly speaking those rights belong to the child and not the parent. However a person with parental responsibility would normally exercise those rights on behalf of a pupil too young to understand those rights (usually meaning those under 13). A child of any age can however ask a parent or a third party to make a SAR on their behalf.

Where the request is made for a child over the age of 13 the School will request that pupil's signed authority to release that information to a third party.

What are the time limits for compliance?

UK-GDPR requires a response to a SAR within a calendar month starting on the date that the SAR is received (or the date on which the information referred to is received if this is later). Where the request is particularly complex and numerous the School can extend that deadline to two months but must write to inform the requester within the original calendar month deadline explaining why the extension is necessary. The School however will not unnecessarily delay the provision of this information and will begin to collate the information as soon as is practicably possible.

What should happen when the School receives a SAR?

All members of staff should be aware of the process for dealing with a SAR. Any request for information on an individual should be sent in the first instance to the Bursar who has overall responsibility for compliance with the DPA. The written request will be acknowledged at this point and the date that the request was received logged.

Depending on the nature of the request and who it is made by or on behalf of, the Bursar will then select the appropriate individuals to begin searching the School's data. If the request for personal data is 'manifestly unfounded or excessive' the Bursar, on behalf of the School, may ask for additional information to enable the School to comply with the request, may request a reasonable charge for compliance (only

appropriate where there would be an excessive cost in responding to the request), or in exceptional circumstances refuse to comply (generally only where the request has been repetitively).

The School's database system, SIMS, has a tool which will allow all data to be extracted in a user friendly format and this would normally be the first step in responding to a SAR. If necessary and appropriate the School's email servers would then be searched for data relating to the requester or the person on whose behalf they are acting. Simultaneously the School will also complete a search of the relevant hard copy records which may include archives if appropriate or relevant.

During this process the Bursar will monitor the timeline to ensure that data is disclosed within the specified timeframe.

What needs to be searched to complete a SAR?

All electronic systems that are under the School's control which include email accounts where these are used on School business. Under the current DPA this includes hard copy records where they are sufficiently well organised to give easy access to specific information about an individual such as a member of staff's personal file.

What Information has to be disclosed?

A SAR only provides access to an individual's own 'personal data' and this means anything that relates to an identifiable, living individual. This does not mean that an individual necessarily has the right to access whole documents so for example an email chain may not always be personal data of the person mentioned in the subject line. Whilst a requester may expect full document disclosure they may not have the automatic right to see it.

Where the data also includes the personal data about another person the School is not obliged to disclose this unless:

- The third party has consented; or
- It is reasonable taking into account all the relevant circumstances to disclose without their consent.

Are there any exemptions to the SAR?

Certain information is exempt from disclosure if it:

- Is legally privileged
- Records the intentions of the School in negotiations with the individual making the SAR
- Consists of a confidential reference *given* by the School (reference received by the School are not subject to the same exemption)
- Consists of exam or test answers or exam results before the allotted publication time;
- Is held for the purpose of management planning (e.g. redundancy planning)
- Would prejudice the prevention and detection of crime if disclosed (such as a live investigation)
- Might cause serious harm or distress in a limited social work context

How is the data to be disclosed?

It does not matter how the data is delivered as long as it is intelligible to the requester – it could be compiled in a table, a single document, or scanned or photocopied from originals and sent digitally or hard copy.

The School will be mindful of the sensitivity, volume and nature of the data and will ensure that it is provided to the requester in the format agreed. Where possible the School will agree with the requester the time and method of delivery to ensure that it reaches them securely. Where the data is particularly

sensitive or there is a large volume of data it will normally be collected in person by the requestor or sent by courier if that is not possible.