St Mark's West Essex Catholic School

DATA PROTECTION POLICY

Date Reviewed:	**November 2018**
Next Review Date:	**November 2020**
Committee:	**Curriculum, Pupils and Admissions**

1 Introduction

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2 Policy Objectives

St Mark's as the Data Controller will comply with its obligations under the GDPR and DPA. We are committed to being concise, clear and transparent about how we obtain and use personal information and will ensure data subjects are aware of their rights under the legislation.

All staff will have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that St Mark's and all staff comply with the legislation.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

St Mark's collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

The Principles

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Transfer Limitation

In addition, personal data shall not be transferred to a country outside the EEA 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 as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[1].

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Basis for processing personal information

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school

- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which the data controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[2]

- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interest's assessment must be carried out and recorded.

Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited[3] unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:

(a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject

[2] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

[3] GDPR, Article 9

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent

(d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim

(e) the processing relates to personal data which are manifestly made public by the data subject

(f) the processing is necessary for the establishment, exercise or defence of legal claims

(g) the processing is necessary for reasons of substantial public interest

(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services

(i) the processing is necessary for reasons of public interest in the area of public health.

St Mark's privacy notice sets out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless St Mark's can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

Responsibilities under Act

All staff have a duty to observe the principles of the Act. (See section 4 page 5). These guidelines are intended to assist staff to understand the aims and principles of the Act and to set out the main areas in which staff are likely to be affected by data protection issues in the course of their work.

Governing Body

The Governing Body has responsibility for:

- Ensuring the implementation of the General Data Protection Act.
- Ensuring that school policies, procedures and practice are consistent with the objectives of the policy.
- Ensuring that complaints are investigated and dealt with effectively.
- Ensuring that appropriate training takes place for the Headteacher and all staff.

Headteacher

The Headteacher is responsible for:

- Ensuring that the General Data Protection policy is implemented in the schools procedures and practices.
- Ensuring that the procedure is brought to the attention of all employees and that all staff receive appropriate training.

- Compliance with the procedure at a practical level through action in recruitment and selection, training and development and general management.
- Encouraging good practice by all staff and dealing appropriately with breaches of the Act.

Data Controller

The Governing Body is the school's Data Controller. Where the Governing Body considers it appropriate a designated person may be nominated to act as Data Protection Officer (Mr Taylor, Associate Headteacher)to help ensure compliance within the school. The Data Controller is responsible for:

- Implementing and monitoring staff and other data subjects when processing data.
- Providing advice on the aspects of data protection.
- Determining the purposes for which and the manner in which any personal data is, or is to be, processed.

All Staff

Staff must ensure they understand how their work is affected by the General Data Protection Act and abide by the principles of the Act. All staff must assess the information used in the course of their work and their responsibility for any personal data. Failure to abide by the requirements of the Act is a criminal offence and an individual may be held personally responsible for any non-compliance.

It is a condition of employment that employees will abide by the rules and policies made by the school from time to time. All staff must be aware of and ensure that they comply with this procedure.

If there are any questions regarding the General Data Protection Act and its implications please contact Pat Seager (School Governor – Mr Gleeson, nominated data protection officer).

Privacy Notice

St Mark's will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the DPO, how and why the School will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. St Mark's will also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

St Mark's will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

St Mark's will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.

Individual Rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed (see the relevant privacy notice)

- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request (see Appendix 1 - Procedure for Access to Personal Information)

- To have data corrected if it is inaccurate or incomplete

- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim

- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)

- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

- To withdraw consent to processing at any time (if applicable)

- To request a copy of an agreement under which personal data is transferred outside of the EEA.

- To object to decisions based solely on automated processing, including profiling

- To be notified of a data breach which is likely to result in high risk to their rights and obligations

- To make a complaint to the ICO or a Court.

Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Information Security

St Mark's will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

St Mark's will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored

- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform the DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Training

St Mark's will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

St Mark's takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact the school's DPO.

Dealing with Access Requests

St Mark's will comply with requests for access to personal information as quickly as possible and will ensure that requests for access are dealt with within the timescale specified by legislation.

Request for access made by pupils and parents will be dealt with within 15 school days. The school will process requests from all other data subjects within 40 days. An initial response will be sent to the requestor within twenty-one days of receiving an access request. The response will confirm the request has been complied with, indicate the intention to comply, or give the reasons for regarding the request as unjustified.

If, for any reason, these timescales cannot be met, the reason will be explained in writing to the individual making the request.

Any person wishing to exercise their right of access should obtain a copy of the school's access to information form (see Appendix 2 for sample form).

Disclosure of Data

The following attempts to illustrate when data can be disclosed. This list is not exhaustive.

Staff who need to know

Data will be disclosed to members of staff who need to know it in order to carry out their normal duties. However, only that data required will be disclosed.

Purposes specified

Data will only be disclosed for use within the purposes originally specified when it was collected. Any other use amounts to unlawful processing. For example, if information is collected in order to pay school uniform grants in 2002 the school will not be allowed to use that information as a mailing list for a library service.

Specific agreement of data subject

Data will be disclosed to a third party if the data subject has given specific consent, ideally in writing. In such cases, consent will be obtained prior to the disclosure.

Telephone enquiries

Requests from third parties are often made by telephone, with the added problem of verifying the identity of the caller. Even when the call appears to be genuine, data will not be disclosed. Instead, an offer will be made to contact the data subject concerned, on behalf of the caller, or to pass on a message.

Police

Disclosures to the Police are not compulsory except in cases where the school is served with a Court Order requiring information. However, requests from the police for access to information will normally be agreed although the Headteacher may ask for the request to be made in writing. In cases where the school has not been served with a Court Order but receives a request, consideration must be given to the implications of disclosure before any action is taken. The school may be required to provide explanation for any disclosure of the data subject's personal information at a later date and must be able to provide justifiable reasons for doing so e.g. where the school believes that failure to release the information would prejudice an investigation.

Third Party Disclosures

There are a number of circumstances under which data can be disclosed to a third party without the consent of the data subject.

The circumstances are set out in the Act as follows:

- Data required by law – for example data supplied to statutory bodies.
- Data that is in the vital interests of the data subject – for example in a life or death situation.
- Data that would prevent harm to a third party.
- Data that would prevent a crime.
- Data that would be in the interests of national security.

Even in these circumstances, proof of identity, confirming name and address and a request in writing, will be required where practicable. Where the information requested is that of a pupil the requestor must also provide evidence of their relationship to the child. Access requests to educational records may only be made by the child's parent/legal guardian.

Recruitment and Selection

It is important to ensure that applicants who are responding to job advertisements or completing application forms know exactly to whom or where they are supplying their information and for what their information will be used. Only information relevant to the recruitment decision should be requested. Applicants should have explained to them as early as possible what verification checks may be undertaken. This is currently covered in the application form where the individual is requested to sign a declaration of consent.

Before attempting to obtain any information from a third party, for example for the purpose of confirming qualifications or employment history, it is necessary to obtain a signed consent form or some similar form of consent from applicants (this is currently covered in the declaration of consent on the application form). Information should not be sought from applicants unless it can be justified as being necessary to enable the recruitment decision to be made, or for a related purpose such as equal opportunities monitoring. For example, there is no obvious reason why the school should ask applicants for information about their membership of a trade union.

It is important to ensure that personal data used during, and retained after the interview process, is justifiable against any challenge of it being relevant and necessary. St Mark's may be asked to prove that the non-selection of a candidate was on the basis of something other than a discriminatory attitude held by the interviewer. Applicants will have subject access rights regarding interview notes taken. It is for this reason that all interview notes must be legible and understandable. It is recommended that interview notes be kept for a period of 6 months after the date of interview.

DBS checks (SD2 forms)

The school will require all short-listed applicants for all posts to declare criminal convictions, which are 'spent' or 'unspent' and including any cautions, and pending prosecutions. Such declarations will be made on the relevant self-declaration form (SD2) and will be submitted, in a sealed envelope, marked private and confidential, to the Chair of the selection panel or nominated Human Resource Officer, prior to interview. This information must only be disclosed to those that are authorised to see it in the course of their duties.

Information received via a Form SD2 'disclosure of criminal convictions (spent and unspent)' or a 'CRB disclosure application form' must be treated as strictly confidential and only considered in relation to the post being applied for.

Once a recruitment (or other relevant) decision has been made, disclosure information should not be kept for any longer than is necessary. For those applicants who are not appointed this should generally be for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. Once the retention period has elapsed, the school must ensure that any disclosure information is destroyed by secure means, e.g. by shredding.

For successful applicants the SD2 form should be kept securely in the individual's personal file. Disclosure information must only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Confidential References

The General Data Protection Act allows data subjects to access references about themselves *received* by the school (subject to respecting the confidentiality of third parties), but not those *provided* by the school.

Although confidential references received by the school are not exempt from the right of access, consideration must be given to the data privacy rights of the referee. Information contained in, or about, a confidential reference need not be provided in response to a subject access request if the release of this information would identify an individual referee unless:

- The identity of the referee can be protected by anonymising the information,
- The referee has given his/her consent, or
- It is reasonable in all the circumstances to release the information without consent.

The school may not refuse to disclose references received from third parties without providing reasons e.g. the referee may have refused permission for the information to be made available, or the disclosure may result in harm to the referee.
In cases where a confidential reference discloses the identity of an organisation, but not an identifiable individual, as referee, disclosure will not breach data privacy rights.

Confidential references written by St Mark's are exempt from subject access requests. However, the school is recommended to adopt an open reference policy whereby the information contained within a reference is shared with the data subject on request. This helps alleviate any cause for concern by the data subject at a later date.

When writing a reference it must be kept in mind that the details of the reference may, at a later date, be disclosed to the individual (for example by the new employer). The school must ensure that all information provided is up to date and accurate.

Where a reference requests it, the school can disclose information regarding the number of day's sickness of a data subject. However, detailed information about the data subject's health or sickness record (including reasons for absence), falls within the definition of 'sensitive personal data' and must only be disclosed with the explicit (i.e. written) consent of the data subject.

Education Records

The Act sets out specific rights of access for school pupils to their educational records. Educational records are the official records for which Headteachers are responsible. All current and former school pupils, regardless of age, have a right of access to their official educational records held within the school. While in principle pupils have a right of access to the whole of their educational records, in exceptional cases some information may be withheld. The main exemptions are for information which might cause harm to the physical or mental health of the pupil or a third party, information which may identify third parties (for example other pupils), and information which forms part of some court reports. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.

Examination Results

The school must ensure that strict confidentiality and secure office practices are followed while papers are being marked and while results are being compiled. The Act does not give pupils the right to access their own examination scripts but it does allow access to comments made upon them by examiners. However, pupils are able (under subject access rights) to see the breakdown of marks awarded for particular questions, or sections of examinations.

Examination marks should not be shared (either verbally or in writing) with any other person unless the individual pupil has given their permission e.g. the displaying of examination results on a school notice board, or a list sent around the classroom is prohibited.

Home Addresses and Telephone Numbers

Home addresses or telephone numbers of staff or other data subjects must not be given out to third parties unless the individual has given permission to do so.

Alternative approaches include taking the caller's contact details and advising that a message will be passed on requesting that the caller is contacted, or offering to forward correspondence to a pupil or a member of staff on behalf of the caller.

It is important to take care when handling such requests. An individual's pupil/staff status is personal data. The school should be careful to neither confirm nor deny that the person is a pupil or member of staff at the school, or that the person is otherwise known to the school.

E-mail Addresses

Personal and/or work email addresses must not be disclosed. If asked to disclose another member of staff's personal email address, the caller can be asked to give their email address and told that it will be passed on to the individual they are trying to contact 'if' they are a member of the school. It is not appropriate to disclose a colleague's work details to someone who claim they wish to contact them regarding a non-work related matter.

Sickness and Accident Records

Sickness and accident records will include information about an employee's physical or mental health. These types of record should be treated as sensitive personal data and are therefore subject to specific extra requirements under the Act.

The Act makes a distinction between sickness, accident and absence records. Sickness and accident records contain details of the illness, condition or accident suffered by the individual. Absence records however, may explain the reason for the absence as 'sickness' or 'accident' but do not include any reference to specific medical conditions. The information commissioner recommends that sickness and accident records should be separated from absence records and that sickness and accident records should not be accessed where records of absence could be used instead.

In order to hold these records, the school has to satisfy at least *one* of the conditions for processing sensitive personal data,

Those conditions that may be most directly relevant to sickness and accident records are:

- The processing is necessary for the purposes of the exercising or performing of any right or obligation, which is conferred or imposed by law on the school in connection with

employment. This could include obligations under health and safety legislation or for the purpose of administering statutory sick pay. This condition may also be relevant to the need to maintain sickness records so that the school can ensure that an employee is not dismissed on sickness grounds, when it would have been unfair to do so.

- The processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. This condition may therefore apply where the school is defending itself against tribunal or court proceedings.
- The data subject has given his or her explicit consent to the processing. This will only apply where the employee understands what personal data is involved and has given a positive indication of agreement (such as a signature). The consent must also be freely given and not made subject to a detriment if the employee withholds their consent.

Being known as an employee of the school may mean being asked for information, for instance by parents about a member of staff who is off sick. Although this can be awkward, parents must be informed that employees are unable to discuss confidential school matters. Persistent enquiries must be referred to the Headteacher.

Pension and Insurance Schemes

Pension schemes, private medical and permanent health insurance schemes are typically administered by St Mark's but provided or controlled by third parties. Data required to administer such schemes should not be used for other purposes and any data passed to the scheme providers should be limited to that which is necessary to operate the relevant scheme. It should be made clear to employees who join these schemes what data will be passed between the employer and the scheme controller and for what purposes this will be used.

1.1 Photographs, Videos and CCTV

Where it is wished to take photographs or make video recordings of staff and/or pupils, as individuals, as small groups or organised groups, the individual(s) concerned must give their consent and be informed of the purpose(s) for which the information is to be used. For general photographs or video recordings of the school grounds and public places, whereby individuals can not be identified, consent is not required. If the school intends to record a school event such as a sports day or school play, parents must be informed of the intention and the purpose(s) for which the recording will be used. A parent may chose to withdraw their child from such an event if they object to the recording.

The school must ensure the recorded images are stored securely, where only a limited number of authorised persons have access to them. The recorded images must only be retained long enough for any incident to come to light (e.g. for a theft to be noticed). The school may disclose recordings to a law enforcement agency in order to help with the prevention or detection of crime (see section 8.5) but must not release the images to any other third party.

For further guidance on the use of CCTV please refer to the Information Commissioners website under 'codes of practice our response and other papers'.

Equal Opportunities Monitoring

The Act specifically allows for processing of data on racial or ethnic origin, religion and disability if it is necessary for keeping under review the existence, or absence, of equality of opportunity. The collection of this information is exclusively used for the statistical evaluation of the school's equal opportunities policy within recruitment and employment.

The school, where possible, will ensure anonymity of information when meaningful monitoring is required. The equal opportunities monitoring form, which collects information for this purpose, must be removed from all applications before any assessment of suitability for the post is considered.

Discipline, Grievance and Dismissal

Employees have the same rights of access to files containing information about disciplinary matters or grievances about themselves as they do to other personal data held, unless this information is associated with a criminal investigation, in which case an exemption might apply. All of the normal data protection and access obligations apply to data created or accessed in the course of dealing with disciplinary and grievance issues. Any information referring to a third party must be removed or anonymised before access is granted.

Disciplinary warnings typically 'expire' after one year provided that no further warnings have been issued and no disciplinary action has been taken against the employee during that period. In these circumstances, the warnings will generally be disregarded for future disciplinary purposes but not removed from the personal file. There may be occasions, however, for example in the case of gross misconduct, or gross negligence, where the nature of the offence does not make it desirable and practicable for the one year time limit to apply. If this is so, the employee must be notified in writing when the warning is given of the period applicable, which will not normally exceed 5 years. Exceptions to the time limit will apply where child protection issues are raised - refer to the Child Protection procedure for further information.

Details regarding information relating to discipline/grievance issues must not be disclosed to a third party. For example, being known as an employee of the school may mean being asked, for instance by parents, about the alleged suspension of another member of staff. Under no circumstances should this information be disclosed or confirmed and persistent enquiries must be referred to the Headteacher.

The Internet

Data placed on the school's web site and made available via the Internet will be available in countries which do not have a data privacy regime considered adequate by the EU. Where the school wishes to make staff/pupils personal data available in this way, the consent of the staff and/or pupil(s) concerned must be obtained. Consent can be withdrawn at any point.

Collecting Personal Information

Before collecting or processing personal information the school must consider whether the information collected on staff and other data subjects is necessary for the employment relationship. For example, information concerning an employee's life outside work is unlikely to be necessary. However, it might be legitimate to request information about an employee's other jobs where there is a justifiable need, for example, in connection with Working Time Regulations, or to request information about their children in connection with an application for parental leave.

APPENDIX 1

The following table illustrates, for guidance purposes, the length of time records need to be kept for legal reasons (This is not an exhaustive list. Medical records are kept for a variety of health and safety reasons and will carry various retention times).

Type of Data	**Suggested Retention Period**	**Reason**
Personnel files including training records and notes of disciplinary and grievance hearings	7 years from the end of employment	References and potential litigation
Staff application forms/interview notes	At least 6 months from the date of the interview	Time limits on litigation
Facts relating to fewer than 20 redundancies	3 years from date of redundancy	As above
Facts relating to 20 + redundancies	12 years from date of redundancy	Limitation Act
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax [Employment] Regulations
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay [General] Regulations
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay [General] Regulations
Wages and salary records	6 years	Taxes Management Act
Accident books; records and reports of injuries and diseases	At least 3 years after the date of the last entry	Social Security (Claims and Payments) Regulations; RIDDOR
Health records	During employment	Management of Health and Safety at Work Regulations

Health records where reason for termination of employment is connected with health, including stress-related illness	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations	40 years	COSHH Regulations
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiation's Regulations
Education records, including academic achievements and conduct	At least 6 years from the date the pupil leaves, in case of litigation for negligence	Limitation period for negligence

APPENDIX 2

St Mark's West Essex Catholic School

GENERAL DATA PROTECTION ACT 2018 - DATA SUBJECT ACCESS REQUEST FORM

Under the General Data Protection Act 2018, an individual is entitled to ask for information the school holds about her/him. This entitlement is known as the "Right of Access to Personal Data."

In exercise of the rights granted to me under the General Data Protection Act 2018, I request that the St Mark's West Essex Catholic School provides me with details of the personal data it holds about me and the purposes for which it is used.

I am aware that, under the General Data Protection Act 2018, the school is not obliged to comply with my request unless they are supplied with such information as they may reasonably require in order to satisfy themselves as to my identity and to locate the information which I seek.

DATA SUBJECT (please use BLOCK CAPITALS)

Full Name……Date of birth……

Address ……..……...

...…….……Post code……

Telephone no……..… Length of time at this address ……yrs……mnths

Previous address(es) with dates (if data is required for this period)

...……..……
……..……

Declaration – please complete section (a) and either section (b) or (c)

Section (a) (please tick)

I am providing proof of identity through:

- ❑ my driving licence
- ❑ passport
- ❑ birth or marriage certificate
- ❑ benefit book

and confirmation of my current permanent home address is provided through:

- ❑ the same document
- ❑ a current utility bill in the same name as my birth/marriage certificate

And either section (b) I confirm that I am the Data Subject.

Signed…… Date……..

Or section (c) I confirm that that I am acting on behalf of the data subject and have submitted proof of my authority to do so.

Signed…….. Date…….

Full Name……Date of birth……..…….

Address……...……

……Post code…….……

Tel no……..……...

INFORMATION REQUESTED

Please complete the section below to enable the school to locate the information that you require.

INFORMATION REQUESTED (please use BLOCK CAPITALS, provide as much detail as possible and continue on separate sheet if necessary)

If you would like to provide us with other information on the data you are seeking, please use this space. If you want information that relates to a specific time period or experience, the details would help us to focus our search and respond more quickly.

……..……
……..……
……..……
……
……
……
……
……
……
……
……
……
……

Please return completed form with proof of identity and address to the Headteacher

APPENDIX 3

Key Definitions

Data Controller	The School/Governing Body will normally be the data controller. A 'data controller' is any person/authority who makes decisions with regard to particular personal data, including decisions about the purposes for which the data is to be processed and the way in which that processing takes place.
Data Subject	A 'data subject' is any living person who is the subject of personal data.
Data Subject Access	This is the right of an individual to see personal data relating to him or her that is held by a data controller.
Processing	This term covers almost any conceivable use of data, including obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying the information or data. This means, for example, that simply possessing data constitutes processing for the purposes of the Act. Some examples of processing: Filing, copying a disk, typing an email, deleting an email, archiving files, accessing details from a file, transcribing the contents of a tape, moving a filing cabinet that is full of files, shredding a file, using a camcorder, making a voice recording, keeping a list of contact names and addresses in a diary, keeping ad-hoc information about members of staff.
Structured Manual Filing System	This means any structured set of information which is organised either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual can be easily found.
Manual Records	The Act extends the definition of 'data' from that held in computer-based systems to include all information recorded manually as part of a 'relevant filing system'. It is important to remember that guidance from the Information Commissioner indicates that this definition will be interpreted broadly.

Data	'Data' means information which, • Is being processed by means of equipment operating automatically in response to instructions given for that purpose, • Is recorded with the intention that it should be processed by means of such equipment, • Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or • Does not fall into any of the above categories but forms part of an accessible record.

Personal Data	Personal data means data which relate to a living individual who can be identified from that information.
Non Sensitive Data	General personal details, such as name and address. Details about class attendance, marks and/or grades and associated comments. Reports and references. Notes of personal supervision, including matters about behaviour and discipline.
Sensitive Personal Data	Personal data consisting of information as to a person's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life or the commission or alleged commission of any offence (or proceedings for those offences) by that person. Examples of when sensitive personal data may need to be recorded include: the recording information about dietary needs, for religious or health reasons prior to taking pupils on a field trip, recording information that a staff member is pregnant, as part of pastoral duties or equal opportunity monitoring forms as part of the application process.