ST VINCENT DE PAUL CATHOLIC PRIMARY SCHOOL

Data Protection Policy

includes the School's

Data Security Policy

(Appendix 1: Page 21)

(This document has been produced for schools who have subscribed to Herts for Learning's GDPR toolkit – last updated March 2023)

Mission Statement

"We are called to be the hands and face of Jesus as we learn love and grow together"

Reviewed Summer 2023
Thereafter reviewed bi-annually Summer 2025
Reviewed by: Resource Committee

Signature:  Chair of Governors Date ratified: 4th July 2023

1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that St Vincent de Paul Catholic Primary School (the "School") and its governors and employees are informed about, and comply with, their obligations under the Data Protection Act 2018 (DPA 2018), UK General Data Protection Regulation (UK GDPR) and with other Data Protection legislation.

1.2 The School is a voluntary aided school and is the Data Controller for all the Personal Data processed by the School.

1.3 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will Process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

1.4 The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents / carers and other members of pupils' families, governors, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK GDPR and other legislation. The UK GDPR imposes restrictions on how we may use that information.

1.5 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the UK GDPR may expose the School to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the School's employees. At the very least, a breach of the UK GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

2. Status of the policy

This policy has been approved by the Governing Body of the School. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3. Data Protection Officer[1]

3.1 The Data Protection Officer (the "DPO") is responsible for ensuring the School is compliant with the UK GDPR and with this policy. This post is held by Sally Lorimer, (School Business Manager). In addition, two Deputy DPO will be appointed by the School (Val Hargrave and Trudie Batty). These identified personnel will be jointly known as the 'DPO Team'. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO (email gdpr@stvincent.herts.sch.uk)

3.2 The DPO will play a major role in embedding essential aspects of the UK GDPR into the School's culture, from ensuring the data protection principles are respected to preserving data subject rights, recording data processing activities and ensuring the security of processing.

3.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the UK GDPR requires that DPOs are provided with the

necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

3.3.1 senior management support;

3.3.2 time for DPOs to fulfil their duties;

3.3.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;

3.3.4 official communication of the designation of the DPO to make known existence and function within the organisation;

3.3.5 access to other services, such as HR, IT and security, who should provide support to the DPO;

3.3.6 continuous training and sufficient resources to enable the DPO to meet their UK GDPR obligations;

3.3.7 where a DPO team is necessary, a clear infrastructure detailing roles and responsibilities of each team member;

3.3.8 whether the School should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

3.4 The DPO is responsible for ensuring that the School's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the School must ensure the independence of the DPO.

3.5 The School will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the Governing Body.

3.6 The requirement that the DPO reports directly to the Governing Body ensures that the School's governors are made aware of the pertinent data protection issues. In the event that the School decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

3.7 The DPO will operate independently and will not be penalised for performing their task.

3.8 A DPO appointed internally by the School is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with their role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.

3.9 In order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing personal data. Senior management positions such as chief executive, chief financial officer, head of marketing, head of IT or head of human resources positions are likely to cause conflicts. Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

3.10 In the light of this and in the event that the School decides to appoint an internal DPO, the School will take the following action in order to avoid conflicts of interests:

3.10.1 identify the positions incompatible with the function of DPO;

3.10.2 draw up internal rules to this effect in order to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate;

3.10.3 declare that the DPO has no conflict of interests with regard to his or her function as a DPO, as a way of raising awareness of this requirement;

3.10.4 include a more general explanation of conflicts of interests; and

3.10.5 include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.

3.11 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO.

4. Definition of terms

4.1 **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

4.2 **Consent** of the Data Subject 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 relating to him or her;

4.3 **Data** is information which is stored electronically, or in paper-based filing systems or other media;

4.4 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

4.5 **Data Controllers** means 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.

4.6 **Data Users** include employees, volunteers, governors whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;

4.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

4.8 **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

4.9 **Personal Data** means 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;

4.10 **Personal Data Breach** means 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;

4.11 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR;

4.12 **Processing** means 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;

4.13 **Sensitive Personal Data** means 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.

5. Data protection principles

5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

5.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2 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;

5.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4 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;

5.1.5 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; 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 UK GDPR in order to safeguard the rights and freedoms of individuals; and

5.1.6 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.

5.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

6. Processed lawfully, fairly and in a transparent manner

6.1 The UK GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the School), who the Data Controller's representative is (in this case the DPO), the purpose for which the data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

6.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

6.2.1 where we have the Consent of the Data Subject;

6.2.2 where it is necessary for the performance of a Contract;

6.2.3 where it is necessary for compliance with a legal obligation;

6.2.4 where processing is necessary to protect the vital interests of the Data Subject or another person;

6.2.5 to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects:

6.2.6 where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6.3 Personal data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the DPA 2018. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

6.4 Sensitive Personal Data

6.4.1 The School will be processing Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Personal Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Sensitive Personal Data.

6.4.2 When Special Category/Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph **Error! Reference source not found.** above), a separate condition for processing it must be met. The additional bases which allow processing of Special Category Personal Data are:

6.4.2.1 explicit consent has been given

6.4.2.2 for employment, social security and social protection purposes

6.4.2.3 for vital interests

6.4.2.4 for legitimate activities by a foundation, association or any other not for profit body with political, philosophical or religious or trade union aim

6.4.2.5 for employment, social security and social protection purposes

6.4.2.6 for defence of legal claims

6.4.2.7 for substantial public interest purposes

6.4.2.8 for health and social care purposes

6.4.2.9 for public health purposes

6.4.2.10 for archiving, research and statistics purposes

6.5 Criminal convictions and offences

6.5.1 There are separate safeguards in the UK GDPR for Personal Data relating to criminal convictions and offences.

6.5.2 It is likely that the School will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff and governors or due to information which we may acquire during the course of their employment or appointment.

6.5.3 In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. This information is not routinely collected and is only likely to be processed by the School in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

6.5.4 Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

6.6 Transparency

6.6.1 One of the key requirements of the UK GDPR relates to transparency. This means that the School must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

6.6.2 One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The School has developed privacy notices for the following categories of people:

6.6.2.1 Pupils

6.6.2.2 Parents

6.6.2.3 Staff

6.6.2.4 Governors

6.6.3 The School wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to School premises or if we ask people to complete forms requiring them to provide their Personal Data.

6.6.4 We will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

6.7 Consent

6.7.1 The School must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

6.7.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement 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, then the Consent must be kept separate from those other matters.

6.7.3 In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to obtain Consent from the Parent(s). Consent is likely to be required if, for example, the School wishes to use a photo of a pupil on its website or on social media. Consent is also required before any pupils are signed up to online learning platforms. Such consent must be from the Parent if the pupil is aged under 13.

6.7.4 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 refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.7.5 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Often we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data.

6.7.6 Evidence and records of Consent must be maintained so that the School can demonstrate compliance with Consent requirements.

6.7.7 Consent mechanisms must meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7. Specified, explicit and legitimate purposes

7.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any data which is not necessary for that purpose should not be collected in the first place.

7.2 The School will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

8. Adequate, relevant and limited to what is necessary

8.1 The School will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

8.2 In order to ensure compliance with this principle, the School will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

8.3 Employees must also give due consideration to any forms stakeholders are asked to complete and consider whether the all the information is required. We may only collect Personal Data that is needed to operate as a school functions and we should not collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

8.4 The School will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that the only members of staff or governors who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the School may adopt a layered approach in some circumstances, for example, members of staff or governors may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

8.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the School's data retention guidelines.

9. Accurate and, where necessary, kept up to date

9.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9.2 If a Data Subject informs the School of a change of circumstances their records will be updated as soon as is practicable.

9.3 Where a Data Subject challenges the accuracy of their data, the School will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information

Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

9.4 Notwithstanding paragraph 8.3, a Data Subject continues to have rights under the UK GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 8.3 has been followed.

10. Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed

10.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

10.2 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The School has a retention schedule for all data.

11. Data to be processed in a manner that ensures appropriate security of the Personal Data

11.1 The School has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

11.3 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

11.4 The UK GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our Data Protection Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

11.5 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

11.5.1 **Confidentiality** means that only people who are authorised to use the data can access it.

11.5.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.

11.5.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

11.6 It is the responsibility of all members of staff and governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher or the DPO.

11.7 Please see our Data Security Policy (Appendix 1) for details for the arrangements in place to keep Personal Data secure.

11.8 Governors

11.8.1 Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or parent complaints. Governors should be trained on the School's data protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

11.8.1.1 Ensure that Personal Data which comes into their possession as a result of their School duties is kept secure from third parties, including family members and friends;

11.8.1.2 Ensure they are provided with a copy of the School's Data Security Policy.

11.8.1.3 Using a School email account for any School-related communications;

11.8.1.4 Ensuring that any School-related communications or information stored or saved on an electronic device (including memory sticks) or computer is password protected and encrypted;

11.8.1.5 Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be access by third parties.

11.8.2 Governors will be asked to read and sign a Code of Conduct.

12. Processing in line with Data Subjects' rights

12.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

12.1.1 withdraw Consent to Processing at any time;

12.1.2 receive certain information about the Data Controller's Processing activities;

12.1.3 request access to their Personal Data that we hold;

12.1.4 prevent our use of their Personal Data for direct marketing purposes;

12.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

12.1.6 restrict Processing in specific circumstances;

12.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

12.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;

12.1.9 object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);

12.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

12.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

12.1.12 make a complaint to the supervisory authority (the ICO); and

12.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

12.2 We are required to verify the identity of an individual requesting data under any of the rights listed above. Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

13. Dealing with subject access requests

13.1 The UK GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The School will invite a Data Subject to complete a Subject Access Request Form but we may not insist that they do so. The Form is to help requesters formulate their request and to ensure they provide the necessary details to enable the school to locate more precisely the data that is needed. The Form also requests which format the requester wishes to receive the SAR.

13.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the UK GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent the School from responding to the request as being made under the UK GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the UK GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

13.3 Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is **one calendar month**.

13.4 As the time for responding to a request does not stop during the periods when the School is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing the following measures: a specific GDPR email is available (gdpr@stvincent.herts.sch.uk) and this will be checked regularly (including holiday periods) by the GDPO team.

13.5 The School may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

13.6 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

13.7 Requests from pupils who are considered mature enough to understand their rights under the UK GDPR will be processed as a subject access request as outlined below and the data will be given directly to the pupil (subject to any exemptions that apply under the UK GDPR or other legislation). As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights. In every case it will be for the School, as Data Controller, to assess whether the child is capable of understanding their rights under the UK GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

13.8 Requests from pupils who do not appear to understand the nature of the request will be referred to their Parents or carers.

13.9 Requests from Parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and / or the School considers the child to be mature enough to understand their rights under the UK GDPR, the School shall ask the pupil for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the School to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the School shall not disclose the Personal Data if to do so would breach any of the data protection principles.[2]

13.10 It should be noted that the Education (Pupil Information) (England) Regulations 2005 (the "Regulations") applies to maintained schools so the rights available to parents in those Regulations to access their child's educational records apply to the School. This means that following receipt of a request from a parent for a copy of their child's educational records, the School must provide a copy within 15 school days, subject to any exemptions or court orders which may apply. The School may charge a fee for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a Subject Access Request.

13.11 Following receipt of a Subject Access Request, and provided that there is sufficient information to process the request, an entry should be made in the School's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

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

13.12.1 charge a reasonable fee taking into account the administrative costs of providing the information; or

13.12.2 refuse to respond.

However, this will be discussed first with our legal advisors then the Information Commissioner's Office (ICO), as typically they advise organisations to act with a high level of accountability and transparency, which means co-operating with requesters under most circumstances.

13.13 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request.

13.14 Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

13.15 In the context of a School a subject access request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

14. Providing information over the telephone

14.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the School whilst also applying common sense to the particular circumstances. In particular they should:

14.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

14.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

14.1.3 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

15. Authorised disclosures

15.1 The School will only disclose data about individuals if one of the lawful bases apply.

15.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The School will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

15.2.1 Local Authorities

15.2.2 the Department for Education

15.2.3 the Diocese of Westminster

15.2.4 the Disclosure and Barring Service

15.2.5 the Teaching Regulation Agency

15.2.6 the Teachers' Pension Service

15.2.7 the Local Government Pension Scheme which is administered by Serco

15.2.8 our external HR provider, via Herts for Learning

15.2.9 our external payroll provider, Serco

15.2.10 Our external IT Provider, Herts for Learning HICCS & KeyStageIT

15.2.11 HMRC

15.2.12 the Police or other law enforcement agencies

15.2.13 our legal advisors and other consultants

15.2.14 insurance providers

15.2.15 occupational health advisors

15.2.16 exam boards

15.2.17 the Joint Council for Qualifications;

15.2.18 NHS health professionals including educational psychologists and school nurses;

15.2.19 Education Welfare Officers;

15.2.20 Courts, if ordered to do so;

15.2.21 Prevent teams in accordance with the Prevent Duty on schools;

15.2.22 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;

15.2.23 confidential waste collection companies;

15.3 Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches.

15.4 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

15.5 All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

15.6 The UK GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is Processed ("UK GDPR clauses"). A summary of the UK GDPR requirements for contracts with Data Processors is set out in Appendix 2. It will be the responsibility of the School to ensure that the UK GDPR clauses have been added to the contract with the

Data Processor. Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

15.7 In some cases Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the UK GDPR, including responsibility for any Personal Data Breaches, onto the School. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

16. Reporting a Personal Data Breach

16.1 The UK GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

16.2 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours, unless the data breach is unlikely to result in a risk to the individuals.

16.3 If the breach is likely to result in high risk to affected Data Subjects, the UK GDPR, requires organisations to inform them without undue delay.

16.4 It is the responsibility of the DPO, or the nominated deputy, to decide whether to report a Personal Data Breach to the ICO.

16.5 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

16.6 As the School is closed or has limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects.

16.7 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, our reporting procedures must be followed. In particular, the DPO or such other person identified must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

17. Accountability

17.1 The School must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The School is responsible for, and must be able to demonstrate, compliance with the data protection principles.

17.2 The School must have adequate resources and controls in place to ensure and to document GDPR compliance including:

17.2.1 appointing a suitably qualified DPO (where necessary) and an executive team accountable for data privacy;

17.2.2 implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;

17.2.3 integrating data protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;

17.2.4 regularly training employees and governors on the UK GDPR, this Data Protection Policy, related policies and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The School must maintain a record of training attendance by School personnel; and

17.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. Record keeping

18.1 The UK GDPR requires us to keep full and accurate records of all our Data Processing activities.

18.2 We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

18.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. Training and audit

19.1 We are required to ensure all School personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

19.2 Members of staff must attend all mandatory data privacy related training.

20. Privacy By Design and Data Protection Impact Assessment (DPIA)

20.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

20.2 This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

20.2.1 the state of the art;

20.2.2 the cost of implementation;

20.2.3 the nature, scope, context and purposes of Processing; and

20.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

20.3 We are also required to conduct DPIAs in respect to high risk Processing.

20.4 The School should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including:

20.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

20.4.2 Automated Processing including profiling and Automated Decision-making (ADM);

20.4.3 large scale Processing of Sensitive Data; and

20.4.4 large scale, systematic monitoring of a publicly accessible area.

20.5 We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to pupils. If our processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

20.6 A DPIA must include:

20.6.1 a description of the Processing, its purposes and the School's legitimate interests if appropriate;

20.6.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

20.6.3 an assessment of the risk to individuals; and

20.6.4 the risk mitigation measures in place and demonstration of compliance.

21. Walkie Talkies

21.1 The School recognises the importance of using Walkie Talkies as a method of communication on the site to ensure that children and staff are kept safe at all times. Reasons for using Walkie Talkies are:

21.1.1 to manage behaviour incidents, and to alert staff to attend an incident if required;

21.1.2 for special events such as Sports Days, school fetes, open days, concerts, school plays, etc.; and

21.2 Staff should be aware that when communicating information over a radio network via a Walkie Talkie, it is possible that anyone in the vicinity who is using the same network may be able to overhear conversations. It is important that appropriate controls are in place to prevent individuals without the correct authorisation intentionally or accidentally gaining access to personal information.

21.3 To minimise the risk of unauthorised access to any information that is communicated via Walkie Talkies, staff must ensure that:

21.3.1 under no circumstances must any personal information be communicated which could enable an individual to be identified e.g. use only first name or initials when referring to named persons;

21.3.2 the language used during communications is professional, and that no abusive or inappropriate language is used;

21.3.3 in the event of theft or loss of the equipment, they inform the School's Data Protection team immediately; and

21.3.4 they have completed and understood the appropriate Data Protection and Security training.

22. Policy Review

22.1 It is the responsibility of the Governing Body to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be reported to the DPO.

22.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

22.3 This policy should be reviewed by the School periodically and at least every 2 years. It is important to ensure that the DPO is aware of their obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

23. Enquiries

23.1 Further information about the School's Data Protection Policy is available from the DPO.

23.2 General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Appendix 1: Data Security Policy

1. Policy statement and objectives

The objectives of this Data Security Policy are to ensure that St Vincent de Paul Catholic Primary School and its governors and employees are informed about, and comply with, their obligations under the UK General Data Protection Regulation ("the UK GDPR") and other data protection legislation.

1.1 The School is a voluntary aided school and is the Data Controller for all the Personal Data controlled/processed by the School.

1.2 The purpose of this policy is to inform staff about their specific responsibilities in maintaining and improving security standards and data management, through their working practices and day-to-day interaction with the school's ICT systems.

1.3 We hold personal data on pupils, staff and others to allow the School to conduct its day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can also result in media coverage and potentially damage the reputation of the School, its staff and pupils. Therefore everybody has a shared responsibility to be mindful about data security when they are going about their daily activities and consider how data security risks and threats can be minimised.

1.4 The policy applies to all staff of the School whether temporarily or permanently employed. It also applies to contractors engaged by/working with the School or who have access to information held by the School.

1.5 The School should ensure all staff are aware of and understand the content of this policy. If any staff member is found to have breached this policy, they could be subject to the Disciplinary and Dismissal Policy & Procedure.

1.6 The policy applies to all locations from which School systems are accessed by staff including remote use and the use of portable devices.

2. Status of the policy

This policy has been approved by the Governing Body of the School. It sets out our rules on data security and the legal conditions that must be satisfied in relation to the secure handling, processing, storage, transportation and destruction of personal information.

3. Network/Server Security

Servers should be physically located in an access-controlled environment. Unrestricted access to the computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff or third party support where there is a specific job function need for such access.

The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

Servers should have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification.

Servers should always be password protected, and locked when not in use.

Security-related events should be reported to the IT team and to the DPO. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks, evidence of unauthorised access to privileged accounts.

IT infrastructure such as routers, switches, wireless access points etc. should be kept securely and only be handled by authorised personnel.

Backup Procedures:

i. Backup software must be scheduled to run routinely, as required, to capture all data as required.

ii. Backups should be monitored to make sure they are successful.

iii. A test restoration process will be run regularly.

iv. Backup media must be securely stored.

4. Workstation Security

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorised users, including:

i. Restricting physical access to workstations to only authorised personnel.

ii. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access.

iii. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.

iv. Complying with all applicable password policies and procedures.

v. Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.

vi. Ensuring workstations are used for authorised purposes only.

vii. Never installing unauthorised software on workstations.

viii. Storing all confidential information on network servers.

ix. Keeping food and drink away from workstations in order to avoid accidental spills.

5. Password Security

5.1 Requirements:

i. All system-level passwords (Administrator, etc.) must be changed on a regular 90 days basis, as a minimum.

ii. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. (in most cases they are programmed with 90 prompt to change password)

iii. All user-level and system-level passwords must conform to the standards described below.

5.2 Standards - All users should be aware of how to select strong passwords. Strong passwords have the following characteristics:

- Contain at least eight alphanumeric characters.
- The password is NOT a word found in a dictionary (English or foreign).
- The password is NOT a name or common pattern (e.g. 12345678).
- Passwords should be easily remembered. One way to do this is create a password based on a song title or other phrase, or to string together three random words e.g. coffeetrainfish.
- Passwords could also contain several of the five following character classes *[but we recommend that this should not be enforced]*: Lower case characters; Upper case characters; Numbers; Punctuation; "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/). However, this should only be used in conjunction with the above rules ('P4ssw0rd' is no more secure than 'Password').

5.3 **Protective Measures**

iv. Do not share passwords with anyone. All passwords are to be treated as sensitive, confidential information.

v. Passwords should never be written down, unless securely stored, or stored electronically without encryption.

vi. Do not reveal a password in email, chat, or other electronic communication.

vii. Do not speak about a password in front of others.

viii. Always decline the use of the "Remember Password" feature of applications.

6. Access Control

Staff should only access systems for which they are authorised. Under the Computer Misuse Act 1990 it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

Formal procedures will be used to control access to systems. An authorised manager must request each application for access and access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Staff with management responsibilities must ensure they advise IT of any changes requiring such modification/removal.

Staff should pay particular attention to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals and documentation.

Line managers should ensure that all PC files of continuing interest to the business of the School are transferred to another user before a staff member leaves their employment. It is also good practice for a meeting to be held during which the manager notes all the systems to which the member of staff had access and informs the relevant system administrators of the leaving date. Particular attention needs to be taken when access to personal, commercially sensitive or financial data is involved.

Any contractors (working on site or working remotely via a communications link) to maintain or support computing equipment and software for the School must comply with the terms of this policy and any access control measures with which they are requested to comply with by School staff.

Physical security to all office areas should be maintained. Staff should feel confident about challenging strangers in the office areas without an ID badge.

Clear Desk Policy:

i. Staff are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

ii. Although security measures are in place to ensure only authorised access to office areas, staff members should ensure that documents, particularly of a confidential nature are not left lying around.

7. Security of Portable Equipment and Mobile Devices

Staff using portable computers/laptops must have appropriate access protection, for example passwords and encryption.

Devices must not be left unattended in public places or left in unattended vehicles at any time. Staff are also responsible for the security of the hardware and the information it holds at all times on or off School property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

Staff should always secure laptops, handheld equipment and any removable media when leaving an office unattended and lock equipment away when leaving the office.

Staff working from home must ensure appropriate security is in place to protect equipment or information not be used by non-School staff. This will include ensuring equipment and information is kept out of sight.

Staff should ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team.

Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop and should synchronise all locally stored data with the School network server on a frequent basis.

Mobile Computing and Storage Devices include, but are not limited to: laptop computers, plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or School owned, that may connect to or access the information systems at the School. These devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the IT network. These risks must be mitigated to acceptable levels:

i. Encryption - portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information must use encryption or equally strong measures to protect the data while it is being stored.

ii. Database or portions thereof, which reside on the network shall not be downloaded to mobile computing or storage devices.

iii. Report lost or stolen mobile computing and storage devices immediately to the IT department and the DPO.

iv. Non-departmental owned device that may connect to the School network must first be approved by the IT department.

8. Acceptable Use

While the School network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the systems remains the property of the School.

Staff must pay particular attention to the protection of personal data and commercially sensitive data. All sensitive files must be password protected or encrypted where possible.

For security and network maintenance purposes, authorised individuals within the School may monitor equipment, systems and network traffic at any time.

Authorised staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If staff are in doubt as to whether the individual requesting such access is authorised to do so, they should ask for their identification badge and contact the headteacher. Any authorised staff member will be happy to comply with this request.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of the ICT systems; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

Authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2018 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT systems may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Staff must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

If it is suspected that there may be a virus on any School ICT equipment, staff should stop using the equipment and contact the IT team immediately. They will advise what actions to take and be responsible for advising others that need to know.

It is imperative that staff do not access, load, store, post or send from School ICT system any material that is, or may be considered to be: illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the School or may bring the School into disrepute. This includes, but is not limited to: jokes, chain letters, files, emails, clips or images that are not part of the School business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act or a Subject Access Request.

Where necessary, permission should be obtained from the owner or owning authority and any relevant fees paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

9. Printing, Copying and Transmission of Data

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents emailed, faxed, copied, scanned or printed.

Anyone sending a confidential or sensitive fax should notify the recipient before it is sent.

Staff should ensure that the entire document has copied or printed and check that the copier has not run out of paper. This is particularly important when copying or printing large documents.

Staff should not leave the printer unattended when using it, as another person may pick up the printing by mistake.

When sending data, the most secure method of transmission must be selected, especially where information is particularly sensitive or confidential. All staff should consider the risk of harm or distress that could be caused to the relevant data subject if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

Send only the minimum amount of personal or sensitive information, by whichever method is chosen.

Sending information by email:

i. Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes.

ii. If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list.

iii. Take care when replying 'to all' – do they really all need to receive the information being sent.

iv. If emailing sensitive information, password protect any attachments. Use a separate email or different method to communicate the password e.g. telephone call.

v. When sending sensitive files, consider the use of secure file transfer systems where available, such as Schoolsfx or HertsFX (Hertfordshire schools).

Sending information by post:

- Check that the address is correct.
- Ensure only the relevant information is in the envelope and that someone else's letter has not been included in error.
- Consider using tracking, e.g. recorded delivery or a courier if appropriate.

10. Use of Email

The School gives all staff and governors their own email account to use for all School business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed.

Staff and governors should use their school email for all professional communication.

Monitoring – School employees shall have no expectation of privacy in anything they store, send or receive on the School email system. The School may monitor messages without prior notice.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

Staff should avoid sending or forwarding attachments unnecessarily. Whenever possible, the location path to the file on a shared drive should be sent instead.

Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher.

When emailing confidential/personal data, obtain express consent from a manager to provide the information by email and exercise caution when sending by performing the following checks:

i. Encrypt and/or password protect attachments. Provide the encryption key or password by a separate contact with the recipient(s).

ii. Verify the details, including accurate email address, of any intended recipient of the information. Do not copy or forward the email to any more recipients than is absolutely necessary.

iii. Verify the details of a requestor before responding to email requests for information.

iv. Consider using other secure file transfer methods, such as HertsFX or Schoolsfx (Hertfordshire schools).

v. Request confirmation of safe receipt.

The School email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, sex, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any School employee should report the matter immediately. The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of messages.

- Creating or forwarding "chain letters", "joke" emails, or "pyramid" schemes of any type.

Users should actively manage their email account by:

- Checking emails regularly.

- Deleting all emails of short-term value.

- Organising email into folders and carrying out frequent house-keeping on all folders and archives.

- Activating an out-of-office notification when away for extended periods.

Personal Use - using a reasonable amount of School resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.

The School email account should not be used for personal advertising.

All the above apply whether accessing the School email account onsite, or through webmail or on non-School devices.

11. Data Breaches

The Information Commissioner's Office (ICO) has the power to serve notices requiring organisations to pay up to €20 million or 4% of annual global turnover, whichever is higher, for serious breaches of the UK GDPR and Data Protection Act 2018.

Staff are responsible for:

i. Ensuring that no breaches of information security result from their actions.

ii. Reporting any breach, or suspected breach of security without delay.

iii. Ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

iv. Ensuring they are aware of and comply with any restrictions specific to their role or service area. All staff should be aware of the confidentiality clauses in their contract of employment.

Advice and guidance on information security can be provided by the School's DPO.

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings.

If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, then the actions in the Data Breach Response Plan must be followed. In particular, the DPO must be notified immediately.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

12. Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. The School will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to: the Waste Electrical and Electronic Equipment Regulations 2018, the Data Protection Act 2018, the Electricity at Work Regulations 1989.

The School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

i. Date item disposed of.

ii. Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media.

iii. How it was disposed of e.g. waste, gift, sale.

iv. Name of person and/or organisation who received the disposed item.

Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Appendix 2 – UK GDPR Clauses

The UK GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the UK GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))

2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))

3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)

4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))

5. The Processor must ensure it flows down the UK GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))

6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3)(e))

7. The Processor must assist the Data Controller with their security and data breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))

8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))

9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3)(g))

10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))

11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3))

Appendix 3 – Appropriate Policy Document: Special Category and Criminal Offence Data

Summary

This policy outlines the School's obligations under Data Protection Legislation with regard to the processing of Special Category Personal Data and Criminal Offence Data. This should be read alongside our Data Protection policy, our Data Security policy, and our privacy notices.

This document meets the requirements of the Data Protection Act 2018, that an appropriate policy document be in place where the processing of Special Category Personal Data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security, social protection and for reasons of substantial public interest.

The specific conditions under which data may be processed for reasons of substantial public interest are set out in Schedule 1 to the Data Protection Act 2018 and the School intends to rely on these as and when appropriate.

The School will ensure that all Special Category Data is captured, held and used in compliance with this policy. Any proposed new use of Special Category Data will be subject to a Data Protection Impact Assessment (DPIA). For all uses of Special Category Data, the School will record a description of the lawful basis for processing and confirmation that the appropriate data retention rules are being applied.

Special Category Data

The School is committed to ensuring that all personal data it processes is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The School recognises its duties to protect all personal data but in particular Special Category Personal Data as defined under Data Protection legislation i.e. information that may identify an individual's 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.

Compliance with the Principles of the UK GDPR

Article 5 of the UK GDPR describes 6 principles that we must follow when collecting and using personal information. Where necessary, the School will carry out a DPIA to ensure that processing is compliant with the principles. The following is a summary of our procedures for compliance with those principles regarding Special Category data.

Principle	Procedures for securing compliance
Processed lawfully, fairly and in a transparent manner	The School will: • ensure that such data is only processed where a lawful basis applies; • only process such data fairly, and will ensure that data subjects are not misled about the purposes of any processing; • ensure that processing of such data is described clearly in privacy notices available to all data subjects for transparency.

Principle	Procedures for securing compliance
Collected for specified, explicit and legitimate purposes	The School will: • only collect such data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice; • not use such data for purposes that are incompatible with the purposes for which it was collected, and if we do use the data for a new purpose that is compatible, we will inform the data subject first.
Adequate, relevant and limited to what is necessary	The School will: • only collect and hold such data as necessary for our operational requirements or to meet statutory obligations; • ensure that the data we collect is adequate and relevant.
Accurate and up to date	The School will: • ensure that systems are in place to verify that data is accurate; • ensure that data is kept up to date as necessary.
Kept in a form which permits identification of data subjects for no longer than is necessary	The School will: • ensure data is kept only as long as is necessary for the purposes for which it is collected, or where there is a legal obligation to do so; • where possible, manually delete time-expired data in systems that do not have the functionality to automate disposal.
Processed securely	The School will: • train staff to be particularly aware of the additional risks to Special Category data; • ensure that there appropriate organisational and technical measures in place to protect such data; • take appropriate precautions when transmitting or disposing of the data.

Lawful Bases for Processing

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever we process Personal Data:

- **Article 6(1) (a) Consent**: the individual has given clear consent for us to process their personal data for a specific purpose.
- **Article 6(1) (b) Contract**: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- **Article 6(1) (c) Legal obligation**: the processing is necessary for us to comply with the law (not including contractual obligations).
- **Article 6(1) (d) Vital interests**: the processing is necessary to protect someone's life.
- **Article 6(1) (e) Public task**: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- **Article 6(1) (f) Legitimate interests**: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (*This cannot apply*

to a public authority processing data to perform official tasks, so is generally unlikely to be used.)

Additional Bases for Processing Special Category Data

The additional bases which allow processing of Special Category Personal Data are:

- **Article 9(2) (a)** – explicit consent has been given.
- **Article 9(2) (b)** – for employment, social security and social protection purposes.
- **Article 9(2) (c)** – for vital interests.
- **Article 9(2) (d)** – for legitimate activities by a foundation, association or any other not for profit body with political, philosophical or religious or trade union aim.
- **Article 9(2) (e)** – for employment, social security and social protection purposes.
- **Article 9(2) (f)** – for defence of legal claims.
- **Article 9(2) (g)** – for substantial public interest purposes.
- **Article 9(2) (h)** – for health and social care purposes.
- **Article 9(2) (i)** – for public health purposes.
- **Article 9(2) (j)** – for archiving, research and statistics purposes.

In addition, Schedule 1 of the Data Protection Act 2018 establishes conditions that permit the processing of the special categories of personal data and criminal convictions data. The Schedule is split into four parts:

Part 1 – Conditions relating to employment, health and research

Part 2 – Substantial public interest conditions

Part 3 – Additional conditions relating to criminal convictions

Part 4 – Appropriate policy document and additional safeguards

In most cases, the Special Category data we collect is covered by **Article 6(1) (c)** and **Article 6(1) (e)**, along with **Article 9(2) (g)**. In all cases, we will ensure that we record the conditions for processing any type of Special Category data, as defined in both Articles 6 and 9.