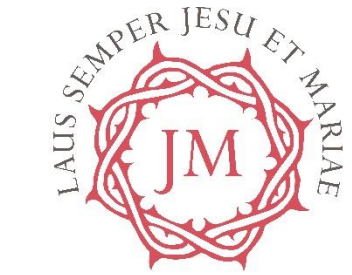

THORNTON

GDPR

DATA PROTECTION POLICY

4.1

DOCUMENT CONTROL

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

Version Number	Date modified	Description of modification	Modified by
1.0	30/1/19	First Draft created for review	S Kurze-Kinton-Heap
1.1	12/2/19	Following a review and meeting with SMT on 8/2/19 amendments made to • make clear distinction between Role of DCL and a DPO. • Make reference to the examinations policy. • Make reference to where the Privacy Policy can be found. • Add deletion and retention information • Make clear processing applied to third party processors who process data on behalf of Thornton College School. • Clarify policy with regards to mark books and student assessment materials. • Clarify Policy regarding taking work home. • Clarify Policy with regards to taking data off site for trips and visits.	S Kurze-Kinton-Heap
1.2	1/3/19	Added further clarification to trips and visits – Pouch for use in exceptional circumstances Camera Policy added to relevant policy list – added to that Policy regarding coloured lanyards to indicate photography consent.	S Kurze-Kinton-Heap
1.3	11/3/19	Added further detail about emergency contact and allergy information in the nursery. Clarified position regarding admissions data and consents for split families.	S Kurze-Kinton-Heap
1.4	26/4/19	Moved Review date to footer Mission Statement added Changed numbering to include total pages in document	S Kurze-Kinton-Heap
1.5	26/6/19	Addition made on page 16 – clause 10.6 regarding deleting and keeping emails	S Kurze-Kinton-Heap
1.6	11/11/19	Clause 11.5.4 amended Screen-Lock timing changed from 2 minutes to 15 minutes after survey of staff with fears over ability to teach effectively if screen locks mid-lesson	S Kurze-Kinton-Heap
2.0	31/7.2020	Review - Updated version number - Updated review dates - Amended 10.1 to include ISBA - Amended Appendix 2 to take whichever guideline is the greater for retention from those sources listed in 10.1 – this was agreed by SMT via email on 8th January 2020 - Removed reference to physical mark books in 11.5.2	S Kurze-Kinton-Heap

3.0	12.8.2021	Review - Amended 4.4 to reflect current practice - Updated references to Union or Member State Law with UK Law to reflect move of UK outside of EU - Added use of OneDrive and Teams where previous references were to the computer network or S Drive - Amended 11.5.2 to remove paper based mark books in line with new approach to use of One Drive - Added reference to completion of Cyber Security Training	S Kurze-Kinton-Heap
3.1	8.12.21	Amended DBS detail after safeguarding update – retention scheduled in appendix on p49	S Kurze-Kinton-Heap
3.2	16.6.22	Amended to make retention period for SARs clear (14.1.7) Amended retention schedule to clarify admissions and to make further edits easier (changed from image to text). Updated to include definition on enquiry and to remove references to data we do not gather e.g Free School Meals	S Kurze-Kinton-Heap-Heap
3.3	22.6.22	Clarified that students over the age of 13 give their own consent – so when taking photographs we will allow a child to remove themselves from a photograph even when a parent has given permission. We will advise students that parents do not want their photograph taken too. Set expectations that we will respond to SARs in a timely fashion but that this may be difficult during school holiday periods	S Kurze-Kinton-Heap
3.4	2.9.22	Added 18.2.5 that Parago now annual sign off mechanism for staff GDPR agreement	S Kurze-Kinton-Heap
3.5	6.12.22	Amended SAR retention to 6 years	S Kurze-Kinton-Heap
3.6	20.4.23	Improved clarity regarding how long images may be used in marketing (response to guidelines) (See section 9 of appendix) Also removed reference to seeking consent before signing up students to learning platforms from 6.7.2 as this is no longer reflective of current practice. Instead a DPIA is conducted before students are signed up for learning purposes – this has been re-phrased to show consent is sought before signing students up for competitions	S Kurze-Kinton-Heap
3.7	24.4.23	Added clarity to retention periods (in appendix) for pre-employment checks in line with changes to recruitment policy	S Kurze-Kinton-Heap
3.8	17.05.23	Added low level concerns procedure/data retention as Section 13.3 and 2.3.1i in data retention appendix	S Kurze-Kinton-Heap
3.9	14.6.23	Clarified retention period of student emails and correspondence. Added 6.2.7 into appendix	S Kurze-Kinton-Heap
4.0	25.08.23	Reviewed and integrated additional information from ISBA guidance document this includes • adding background information at the start of this policy, • added 2.5 • addition of section 4 (application of this policy), • revised wording of section 5, • updates to the definitions in section 6 • revised wording of section 7	S Kurze-Kinton-Heap

		• added section 7.18 care and security • revised wording of section 12 • added 12.10 regarding processing of financial data • revised wording of data subject rights section 15 • revision to section 17 • revision and additions to accountability section 19 • revision to section 20 Record-keeping • revision to section 23 •	
4.1	16.1.24	Review of breach reporting procedures with LSW resulted in changes to section 18 to reflect what happens during non-working hours and the responsibilities of the DCL Also updated section 22 to reflect current practice – the DCL helps to draft DPIAs if needed but the Bursar has final approval for all DPIAs Update 10.2 as it referred to the 'Data Protection' and should say 'the Bursar' Update to 14.1 as it referred to 'insert names and role' also added what happens during non-working hours 14.4 as it did not mention Bursar, also added what happens during non-working hours 15.4 and 15.5 – removed DCL from contact during holidays/weekends and added Executive Team rather than 'SMT' 15.14 and 15.15 amended to Bursar rather than DCL to reflect current practice Amended review date	S Kurze-Kinton-Heap

CONTENTS

Background

Data protection is an important legal compliance issue for Thornton College. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice. The School, as "data controller", is liable for the actions of its staff and trustees/governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

1. MISSION STATEMENT

1.1. 'To educate young people to meet the challenges of life courageously, to use their talents to the full and to live the values of Christ's Gospel'

2. POLICY STATEMENT AND OBJECTIVES

2.1. The objectives of this Data Protection Policy are to ensure Thornton College stakeholders including but not limited to members of our community, governors and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other data protection legislation.

2.2. The School is a Data Controller for all the Personal Data processed by the School.

2.3. 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.

2.4. The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents, guardians, 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 GDPR and other legislation. The GDPR imposes restrictions on how we may use that information.

2.5. 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 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 GDPR could damage our reputation and have serious consequences for the School and for our stakeholders.

2.6. It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

3. 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.

4. APPLICATION OF THIS POLICY

4.1. This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

4.2. Those who handle personal data as employees or [governors/trustees/directors] of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

4.3. In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

4.4. Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

4.5. If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

5. DATA COMPLIANCE ROLES

5.1. The Bursar will endeavour to ensure that personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Neither the Bursar nor Data Compliance Lead (DCL) are Data Protection Officer (DPO) and should not be regarded as such. Reporting to the Bursar, the Data Compliance Lead (the "DCL") co-ordinates data compliance work, communication and record keeping at the School. Any questions or concerns about the operation of this policy should be referred in the first instance to the DCL and the Bursar, should matters need to be escalated they should be brought to the attention of to the SMT or Governors.

5.2. The DCL, under the direction and supervision of the Bursar, will work to embed essential aspects of the GDPR into the School's culture, ensuring the data protection principles are communicated and recording data processing activities.

5.3. The DCL, under the direction and supervision of the Bursar, should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this the DCL and Bursar will required the necessary support and resources to enable to effectively co-ordinate tasks. Factors that should be considered include the following:

5.4. senior management support;

5.5. time for DCL and Bursar to fulfil their duties;

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

5.7. official communication of the designation of the Bursar and DCL to make known existence and function within the organisation;

5.8. access to other services, such as HR, IT and security, who should provide support to the DCL and Bursar;

5.9. continuous training to stay up to date with regard to data protection developments;

5.10. whether the School should give the Burar and DCL access to external legal advice to advise the DCL on their responsibilities under this Data Protection Policy.

5.11. The DCL reports to the Bursar, The DCL will receive advice from the Bursar and the SMT. The Bursar has oversight of the DCL's activities and therefore the Bursar 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 Bursar should report directly to the highest management level for Data Protection matters, i.e. the Governing Body.

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

5.13. A DCL 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 his or her role as DCL. It follows that any conflict of interests between the individual's role as DCL and other roles the individual may have within the organisation impinge on the DCL's ability to remain independent.

5.14. In order to avoid conflicts the DCL cannot hold another position within the organisation that involves determining the purposes and means of processing personal data. Senior

management positions such as Head Teacher, Deputy Head Teacher, Head of marketing, or Head of IT 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 DCLs.In the light of this, the School will take the following action in order to avoid conflicts of interests:

5.14.1. identify the positions incompatible with the function of DCL;

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

5.14.3. include a more general explanation of conflicts of interests; and

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

5.15. 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 DCL or Bursar.

6. DEFINITION OF TERMS

6.1. 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;

6.2. 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;

6.3. Data is information which is stored electronically, on a computer, or in certain paper- based filing systems or other media such as CCTV;

6.4. 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.

6.5. Data Controllers a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its [trustees/directors/governors]) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

6.6. Data Users include employees, community members, 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;

6.7. Data Processors an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

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

6.9. Personal Information (or 'Personal Data') ; any information relating to a living individual (a data

subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

6.10. Personal Data Breach a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6.11. Processing virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.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;

6.12. Special Categories of personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

6.13. 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 person's sex life or sexual orientation.

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

7. DATA PROTECTION PRINCIPLES

7.1. The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

7.1.1. processed lawfully, fairly and in a transparent manner:

7.1.2. Collected for specific and explicit purposes and only for the purposes it was collected for;

7.1.3. Relevant and limited to what is necessary for the purposes it is processed;

7.1.4. Accurate and kept up to date;

7.1.5. Kept for no longer than is necessary for the purposes for which it is processed; and 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 GDPR in order to safeguard the rights and freedoms of individuals; and

7.1.6. Processed in a manner that ensures appropriate security of the personal data

7.2. Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

7.3. One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

7.4. Other lawful grounds include:

7.4.1. compliance with a legal obligation, including in connection with employment, engagement of services and diversity;

7.4.2. contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;

7.5. a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7.6. The 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 DCL reporting to and overseen by the Bursar), 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.

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

7.7.1. where we have the Consent of the Data Subject;

7.7.2. where it is necessary for compliance with a legal obligation;

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

7.7.4. 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.

7.8. 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 Act. 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.

7.9. Sensitive Personal Data

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

7.9.2. When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 5.1 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

7.9.2.1. The Data Subject's explicit consent to the processing of such data has been obtained

7.9.2.2. processing is necessary for reasons of substantial public interest, on the basis of UK law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

7.9.2.3. processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

7.9.2.4. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by UK law or a collective agreement pursuant to UK law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

7.10. The School recognise that in addition to Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

7.11. Biometric Data

7.11.1. The School may decide to process Biometric Data as part of an automated biometric recognition system, for example, for cashless catering or photo ID card systems where a pupil's photo is scanned automatically to provide him or her with services. Biometric Data is a type of Sensitive Personal Data.

7.11.2. Where Biometric Data relating to pupils is processed, the School must ensure that each parent of a child is notified of the school' intention to use the child's Biometric Data and obtain the written consent of at least one parent before the data is taken from the pupil and used as part of an automated biometric recognition system. The School must not process the Biometric Data if a pupil under 18 years of age where:

7.11.3. the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;

7.11.3.1. no Parent has Consented in writing to the processing; or

7.11.3.2. a Parent has objected in writing to such processing, even if another Parent has given written Consent.

7.11.4. The School must provide reasonable alternative means of accessing services for

those pupils who will not be using an automated biometric recognition system. The School will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.

7.11.5. The School must obtain the explicit Consent of staff, governors, or other Data Subjects before Processing their Biometric Data.

7.13. Criminal convictions and offences

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

7.13.2. 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.

7.13.3. 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.

7.13.4. 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.

7.14. Transparency

7.14.1. One of the key requirements of the 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.

7.14.2. 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:

7.14.2.1. Pupils

7.14.2.2. Parents and Guardians

7.14.2.3. Staff and Volunteers

7.14.2.4. Governors and Members of the Community

7.15. The School wish 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.

7.16. 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.

7.17. Consent

7.17.1. The School must only process Personal Data on the basis of one or more of the lawful bases set out in the 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.

7.17.2. 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.

7.17.3. 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). In the event that we require Consent for Processing Personal Data about pupils aged 13 or over, we will require the Consent of the pupil although, depending on the circumstances, the School should consider whether it is appropriate to inform Parents about this process. 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 competitions Such Consent must be from the Parent if the pupil is aged under 13. When relying on Consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us. If a parent has previously given or withheld consent (such as for photography) we will inform the student of their parent's wishes to inform their choice. We will also inform parents if a student over the age of 13 consents to be photographed when they have previously withheld consent.

7.17.4. In the event we are relying on consent, this will be sought from the parent/guardian with whom the parent resides at point of admission to the school. However, if anyone with a parental responsibility for that child wishes to withdrawn consent at any time they may do so by contacting any member of staff.

7.17.5. 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.

7.17.6. 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.

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

7.18. Care and data security

7.18.1. More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

7.18.2. We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to [insert name / role], and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

8. SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

8.1. 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.

8.2. 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.

9. ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY

9.1. 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.

9.2. 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.

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

9.4. 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).

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

10. ACCURATE AND, WHERE NECESSARY, KEPT UP TO DATE

10.1. It is the duty of the Administration team to ensure that 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.

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

10.3. 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 Bursar 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.

10.4. Notwithstanding paragraph 8.3, a Data Subject continues to have rights under the 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.

11. DATA RETENTION

11.1. 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. The school will use the guidelines set out in the UK Government Data Protection Guide for Schools. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf , the ISBA Guidelines for Independent Schools on the Storage and retention of Records and documents (copy in X Drive, GDPR, Policy) and Information Management Toolkit for Schools https://cdn.ymaws.com/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf The relevant sections of both of these documents can be found in the appendices.

11.2. It is the duty of the school health centre team to delete the medical data from relevant

systems/shred paper copies in line with the schedule above. As such an annual review will take place at the beginning of the new year to identify and remove files for deletion.

11.3. It is the duty of the school bursary team to delete the financial data from relevant systems/shred paper copies in line with the schedule above. As such an annual review will take place at the beginning of the new year to identify and remove files for deletion

11.4. It is the duty of the Trip Leader to delete all trip data from relevant systems/shred paper copies in line with the schedule above. As such an annual review will take place at the beginning of the new year to identify and remove files for deletion.

11.5. It is the duty of the school administration team to delete other data from relevant systems/shred paper copies in line with the schedule above. As such an annual review will take place at the beginning of the new year to identify and remove files for deletion.

11.6. It is the duty of the IT team to ensure files deleted from the network are removed from the back-ups in line with the schedule above. As such an annual review will take place at the beginning of the new year to identify and remove files for deletion.

11.7. Emails will be automatically deleted after 60 days. It is the duty of the recipient to ensure that any that may need to be kept for other purposes including but not limited to safeguarding, medical records or invoicing are copied onto the appropriate system i.e CPOMS, ISams or PASS.

12. DATA PROCESSING

12.1. Data to be processed in a manner that ensures appropriate security of the personal data.

12.2. The School have 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.

12.3. The 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. The School must 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.

12.4. 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.

12.5. 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. These measures include but are not limited to:

12.5.1. Keep all electronic records on a secure, password protected system such as the One Drive/MS Teams, S Drive, iSams, SISRA, Firefly or CPOMS.

12.5.2. The default school policy is to store assessment data on iSams and SISRA, if further data needs to be tracked the default locations are Firefly Markbooks, One Drive or the S drive as these are accessed via the school network and backed up. Teachers must not use paper based markbooks without express written consent of the Bursar.

12.5.3. Lock computers when not in use.

12.5.4. Set screensavers on IT equipment to activate after no more than 15 minutes of inactivity and require a password to re-gain access to the device.

12.5.5. Keep all hard copies of data in a locked location (office, filing cabinet, drawer or cupboard) on school premises when not in use.

12.5.6. Shred any hard copies of data that are no longer required, incorrect or out of date.

12.5.7. Not remove any data from the school site in soft or hard copy examples include student progress records and mark books. No member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored.

12.5.8. Not to use USB Drives, Portable hard drives, CDs, DVDs or other electronic media to store or transport data.

12.5.9. No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so

12.5.10. Use of personal email accounts or personal devices by Governors/trustees or staff for official School business is not permitted.

12.5.11. Not to email, fax or post data to others, even those within our organisation without appropriate safeguards such as encryption.

12.5.12. Not to request data to be sent from colleagues via email.

12.5.13. Verify the identity of callers/visitors requesting information via telephone or face to face.

12.5.14. Keep the staffroom door locked at all times

12.5.15. Regularly update passwords in line with the school IT policy, these

should be appropriately complex and not disclosed to others under any circumstances

12.5.16. Complete all recommended cyber security training as communicated by the Bursar and IT team

12.5.17. Only share school IT equipment with other school staff, Governors or members of the community. i.e staff should not allow students, family members or friends to use laptop or tablet devices provided by the school.

12.5.18. Marking: It may not be possible to mark all student work in school during the school day. Therefore, staff are permitted to take student work home to be assesses. Staff must take due care that student work is kept safely at their home and during transit. Staff must not mark in or take student work to a public location examples include but are not limited to a café, waiting room or mode of public transport.

12.5.19. Trips: When accompanying students on a trip or visit, leaders need to take data regarding the students with them in case of emergency or a requirement for medical treatment. Depending on the length of the trip and the infrastructure available in the visit location trip leaders should pick one of the following methods to ensure access to this information when on their visit.

12.5.19.1. Ideally access directly on iSams as this is up to date, password protected, secure and backed up

12.5.19.2. If this is not possible, save it on a shared drive that can be accessed remotely via One Drive or Citrix such as the S: Drive as this is password protected, secure and backed up.

12.5.19.3. If this is not possible, save on the on the staff's own documents area of firefly this is password protected, secure and backed up. It can be accessed from anywhere with an internet connection.

12.5.19.4. If there is concern regarding internet connectivity at the location then this data should be held on a school device such as an ipad, the files should be secured with a password as well as the device. This device should be kept with the member of staff at all times or secured in a suitable location such as a hotel bedroom safe.

12.5.19.5. If there is a concern there will be no access to power, such as on an adventure trip such as World Challenge a lockable pouch will be used to store personal information. Written consent from the Bursar must be attained; this approach is for exceptional circumstances only.

12.6. Data Users must follow all procedures and technologies we put in place 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 Security Policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

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

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

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

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

12.8. It is the responsibility of all members of staff, community members 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 Head Teacher, Bursar or the DCL.

12.9. Where third party processors are used, assurance will be sought that they are compliant with the school GDPR Policy. Depending on the nature of the data held and regularity of processing, these organisations may be asked to either sign a data compliance contract or provide a copy of the GDPR Policy and Written assurance that all data regarding subjects at our school will be subject to the full safeguards outlined in their policy. An electronic log will be kept on the school network in the GDPR folder of third party processors which will include the nature, date and method of confirmation of compliance.

12.10. Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the [Bursar]]. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly

13. GOVERNORS AND COMMUNITY MEMBERS

13.1.1. Governors and Community Members 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' data

protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

13.1.1.1. 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

13.1.1.2. Ensure they are provided with a copy of the School's GDPR Policy.

13.1.1.3. Using a School email account for any School-related communications

13.1.1.4. Ensuring that any School-related communications or information stored or saved on an electronic device or computer is password protected and encrypted.

13.1.1.5. 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.

13.1.1.6. Governors will be asked to read and sign an Acceptable Use Agreement.

14. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

.

14.1. In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data) on a working school day, you must tell the Bursar or DCL as soon as possible.

14.2. Individuals also have legal rights to:

14.2.1. require us to correct the personal data we hold about them if it is inaccurate;

14.2.2. request that we erase their personal data (in certain circumstances);

14.2.3. request that we restrict our data processing activities (in certain circumstances);

14.2.4. receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and

14.2.5. object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

14.3. None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

14.3.1. object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);

14.3.2. object to direct marketing; and

14.3.3. withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

14.4. In any event, however, if staff receive a request from an individual who is purporting to exercise one or more of their data protection rights, they must tell the Bursar or DCL as soon as possible. Where the request is on a non-working day such as a weekend, holiday or bank holiday the member of staff should contact a member of the Executive Team who will co-ordinate next steps.

14.5. 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.

14.6. Low-level concerns about adults

We will process personal data about you, whether or not it constitutes special category data, in accordance with our approach to low level concerns as outlined in our Low-Level Concerns policy. Such records are subject to the rules on retention set out in the school's Low-Level Concerns Policy, and you have the same rights in respect of that information, as any other personal data that we hold on you. However, any requests to access, erase or amend personal data we hold in accordance with this policy may be subject to necessary exemptions, for example if we consider that compliance with the request might unreasonably impact the privacy rights of others or give rise to a risk of harm to children. As a general rule, records of low-level concerns will be kept at least until [or for up to 7 years following] the termination of your employment[1], but may need to be retained longer: e.g. where relevant, individually or cumulatively, to any employment, disciplinary or safeguarding matter.

15. DEALING WITH SUBJECT ACCESS, RECTIFICATION, ERASURE, PORTABILITY OR RESTRUCTION OF PROCESSING REQUESTS

15.1. The GDPR extends to all Data Subjects a right of access to their own Personal Data. They also have the right to request data be erased, amended, sent to another organisation or have restrictions applied to the processing of their data. A formal request from a Data Subject for information that we hold about them can be made verbally or in writing to any member of staff.

15.2. It is important that all members of staff are able to recognise that a 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 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 GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests must be dealt with promptly and in any event within 28 days. NB this includes weekends and holiday periods.

15.3. It is important that all members of staff are able to recognise that a request made by a person for their own information to be amended, erased, sent to another organisation or to limit it's processing, even if the Data Subject does not specifically use these terms or phrases in their request or refer to the GDPR. This should not prevent the School from responding to the request as being made under the GDPR, if appropriate. Requests for information must be dealt with promptly and in any event the requestor must be informed of the schools decision (to comply or refuse the request) within 28 days. NB this includes weekends and holiday periods. The school aim to make the data available within one month of the request, the school may take a further two months to complete an SAR that is complex. SAR

15.4. Any member of staff who receives a request of this nature on a working day, must immediately inform the Bursar or DCL as the statutory time limit for responding is 28 days.

15.5. As the time for responding to a request does not stop during the periods when the School are closed for weekends, bank holidays or 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.

15.5.1. The Bursar should be informed of this request immediately.

15.5.2. If Bursar is unavailable, the Head Teacher or Deputy Head Teacher should be informed of this request immediately who will decide upon, and co-ordinate next steps. Should they be unavailble, then staff should contact any member of the SLT.

15.6. A fee may not be charged to the individual for provision of this information

15.7. 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.

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

15.9. Requests from pupils who are considered mature enough to understand their rights under the 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 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 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.

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

15.11. 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 consider the child to be mature enough to understand their rights under the 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.

15.12. 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, 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 28 days 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.

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

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

15.13.2. refuse to respond.

15.14. 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 Bursar before refusing a request.

15.15. 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 Bursar if you are unsure which exemptions apply.

15.16. In the context of the School a subject access request may be 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.

15.17. Once complete, Subject Access Requests will be available to download for a period of one week (unless requested in hard-copy form). After this time the College will retain a copy of the data for a period of six years from the date the SAR was made available to the subject in case further copies are required. After this time, subsequent requests for copies of the data will be treated as a new subject access request.

16. PROVIDING INFORMATION OVER THE TELEPHONE

16.1. 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:

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

16.1.2. 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.

16.1.3. Refer to their line manager, the Bursar or the DCL for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

17. AUTHORISED DISCLOSURES

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

17.2. 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:

17.2.1. Local Authorities
17.2.2. the Department for Education
17.2.3. the Disclosure and Barring Service
17.2.4. the Teaching Regulation Agency
17.2.5. the Teachers' Pension Service
17.2.6. the Local Government Pension Scheme which is administered by HCC
17.2.7. our external HR provider
17.2.8. our external payroll provider
17.2.9. Our external IT Provider
17.2.10. HMRC
17.2.11. the Police or other law enforcement agencies
17.2.12. our legal advisors and other consultants
17.2.13. insurance providers
17.2.14. occupational health advisors
17.2.15. exam boards including
17.2.16. the Joint Council for Qualifications;
17.2.17. NHS health professionals including educational psychologists and school nurses;
17.2.18. Education Welfare Officers;
17.2.19. Courts, if ordered to do so;
17.2.20. Prevent teams in accordance with the Prevent Duty on school;
17.2.21. other school, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;
17.2.22. confidential waste collection companies;

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.

17.3. 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.

17.4. All Data Sharing Agreements must be signed off by the Bursar, the DCL will keep a register of all Data Sharing Agreements.

17.5. The 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 ("GDPR clauses"). A summary of the GDPR requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the School to ensure that the 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

17.6. 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 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 Bursar for further advice before agreeing to include such wording in the contract.

18. REPORTING A PERSONAL DATA BREACH

18.1. One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

18.2. In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If staff become aware of a personal data breach on a working school day they must notify the Bursar or DCL immediately. If a member of staff discovers a data breach on a weekend, bank holiday or school holiday, they must report this to a member of the Exec Team immediately who will decide if this should be reported. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

18.3. It is the responsibility of the Bursar, to decide whether to report a Personal Data Breach to the ICO and to ensure appropriate mitigating actions are taken

18.3.1. If the DCL is the first to be notified of a suspected Personal Data Breach on a working school day, they will notify the Bursar as soon as possible. If the Bursar cannot be reached within that working day, the DCL will attempt to contact the Head Teacher, if they cannot be reached the DCL will contact the Deputy Head Teacher. In these instances, the Head Teacher or Deputy Head Teacher will decide if the breach needs to be reported and instruct the appropriate members of staff with regards to next steps and mitigating actions.

18.4. 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.

18.5. 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. If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, the Bursar or other available member of the Executive Team must be notified immediately. If they are not available, then any member of the SLT should be contacted. All evidence relating to the potential Personal Data Breach must be preserved.

18.6.

19. ACCOUNTABILITY

19.1. The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

19.1.1. keeping records of our data processing activities, including by way of logs and policies;

19.1.2. documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and

19.1.3. generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

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

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

19.3.1. appointing a suitably qualified DCL to co-ordinate compliance activities reporting to a member of the SMT accountable for data privacy; the Bursar.

19.3.2. 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.

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

19.3.4. regularly training employees and governors on the 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.

19.3.5. Staff are required to read a staff GDPR agreement on an annual basis which reminds them of the key principles of this policy. This is managed and recorded using the Parago system. This requirements does not replace the requirement for

all staff to be aware of the full GDPR policy and attend induction/INSET training.

19.3.6. 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.

20. RECORD KEEPING

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

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

20.3. These records should include, at a minimum, the name and contact details of the Data Controller, 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.

20.4. It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

20.5.

20.6. Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

21. TRAINING AND AUDIT

21.1. 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.

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

22. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

22.1. 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.

22.2. 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:

22.2.1. the state of the art;

22.2.2. the cost of implementation;

22.2.3. the nature, scope, context and purposes of Processing; and

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

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

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

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

22.3.1.2. Automated Processing including profiling and ADM;

22.3.1.3. large scale Processing of Sensitive Data; and

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

22.4. 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.

22.5. A DPIA must include:

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

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

22.5.3. an assessment of the risk to individuals; and

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

23. OTHER POLICIES AND DOCUMENTS

23.1. All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies: exams policy, camera policy, staff code of conduct, IT Policy and privacy statement,. Should you wish to refer to these, copies of all school policies are available from the Head's Personal Assistant. NB the Privacy Statement is also available via the school website.

24. POLICY REVIEW

24.1. 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 DCL via the Bursar.

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

25. ENQUIRIES

25.1. Further information is available in the first instance from the DCL, or the Bursar.

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

26. APPENDIX 1 – GDPR CLAUSES

The GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the 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 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 UK 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 UK law. (Art. 28(3))

APPENDIX 2 : PP 66-67 OF UK GOVERNMENT DATA PROTECTION GUIDE FOR SCHOOLS. Plus Extracts from ISBA Retention of Records and Data. &
APPENDIX 3: INFORMATION MANAGEMENT TOOLKIT FOR SCHOOLS pp37-56 Longer retentions period chosen when these sources do not agree
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf
https://cdn.ymaws.com/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

Management of the School

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies[2]			Date of meeting + 10 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

1.1 Governing Body					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

1.2 Head Teacher and Senior Management Team					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. It is then used for some validation and cross checking of enrolment details. Once enrolled, the child's records in the MIS become the core record. Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it (for example, where in the city children are interested in our school, or the SEN make up) is aggregated within the first year to a level being non-personal, after that, the detailed data within the admission file could be deleted. It is important to retain detailed data for a year, any appeals for which richer data about other successful/unsuccessful appeals may be relevant typically happen in the first year.

1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL When dealing with appeals, having a reasonable history of any other appeals in some detail can be needed to deal with the particular appeal. The information is needed alongside the admissions policies of the time.
1.3.4	Enquiries	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	We believe that someone is an admission or potential admission from the time that pay their registration fee - before this they are an enquiry. That we will keep the details of enquiries until the September that the child would be in year 12 so they can be invited to relevant marketing events/included in campaigns- or if the family ask us to remove them from mailing lists.
1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL

1.3 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Administration					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.13	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	We keep Enhanced DBS certs, self-declarations, interview notes and, if relevant, RAs on the appointment of staff on file. (in line with the staff files destruction) DBS Enhanced certificates are destroyed after 6 months (the top half may be kept); however, the College reserves the right to keep on file DBS certificates containing information that may need to be referred to for safeguarding purposes. This is in line with the Disclosures and Barring Service and the ICO For successful candidates, the School will retain information generated through online searches for the duration of the individual's employment and in accordance with its Retention of Records Policy after employment ends. For unsuccessful candidates, the School retains the information generated from online searches for six months from the date on which they are informed their application was unsuccessful, after which it will be securely destroyed.	SECURE DISPOSAL

2.1.5	Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer’s guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

2.2 Operational Staff Management					
	Basic file description	Data Prot administrative	Statutory Provisions Issues	Retention Period [Operational]	Action at the end of the life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years Keep a permanent record that mandatory checks have been undertaken (but do not keep DBS certificate information itself: 6 months as above)	SECURE DISPOSAL As above, but do not delete any information which may be relevant to historic safeguarding claims. (keep this indefinitely)
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		ISBA Current +7 Years	SECURE DISPOSAL As above, but do not delete any information which may be relevant to historic safeguarding claims. (keep this indefinitely)
2.2.4	Contracts of employment	Yes		7 years from effective date of end of contract	SECURE DISPOSAL
2.2.5	Immigration records	Yes		Minimum – 4 years	SECURE DISPOSAL
2.2.6	Health records relating to employees	Yes		7 years from end of contract of employment	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.1i	Low Level Concerns	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	7 years from the date of the end of employment but may be retained for longer e.g. where relevant, individually or cumulatively, to any employment, disciplinary or safeguarding matter. . Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
	written warning – level 1			Date of warning + 6 months	
	written warning – level 2			Date of warning + 12 months	
	final warning			Date of warning + 18 months	
	case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		7 years from completion of relevant project, incident, event or activity.	SECURE DISPOSAL
2.4.3	Records relating to accident/ injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

1 Employers are required to take a "clear copy" of the documents which they are shown as part of this process

2.5 Payroll and Pensions					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 6 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years. NB ISBA Possibly Permanent depending on nature of scheme – at Bursar's discretion	SECURE DISPOSAL

Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

3.1 Risk Management and Insurance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
3.1.2	Insurance Policies			Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.	
3.1.3	Correspondence related to claims/ renewals/ notification re: insurance			Current year + 7 years	

3.2 Asset Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

2 This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention

3 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice

3.3 Accounts and Statements including Budget Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

Property Management

This section covers the management of buildings and property.

4.1 Property Management					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL

Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes		7 years from the student leaving the school	
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
	Internal			This information should be added to the pupil file	

5.1.3	Behaviour			This is all relevant for managing children when with at your school. 1 year allows a period of ‘handover’ to next institution with conversations supported by rich data if relevant.	
5.1.4	Exclusions			1 year after pupil leaves. Exclusion data should be ‘passed on’ to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.	

5.1 Pupil's Educational Record					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Safeguarding and Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded • Policies and procedures • Accident / Incident reporting • Child Protection files Keep a permanent record of historic policies Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2] If a referral has been made / social care have been involved; or child has been subject of a multi-agency plan; or there is a risk of future claims – indefinitely. [If the school operates a low level concerns policy, if there has been no multi-agency action, consider whether or not the child needs to be named in any record concerning an adult, or if a copy should be kept on the child protection file.]

5.2 Attendance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made. Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child. After that period, non-identifiable summary statistics are all that is required to support longer- term trend analysis of attendance patterns. We noted another GDPR principle here that may apply to attendance. Under data minimisation, where ‘paper records’ capture attendance, this paper record duplicates the electronic version and is probably required once the paper has been transferred to a stable electronic format.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 35 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 35 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 35 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 35 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

Curriculum Management

6.1 Statistics and Management Information					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books and attainment	No		Current year + 1 year 1 year after the pupil has left the school feels proportionate. Trend analysis is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity. After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

6.2.7	Pupil Email Accounts	No		26.1. Students below Year 10 – Will be deleted in line with '10.6 Emails will be automatically deleted after 60 days. It is the duty of the recipient to ensure that any that may need to be kept for other purposes including but not limited to safeguarding, medical records or invoicing are copied onto the appropriate system i.e CPOMS, ISams or PASS.' 26.2. For students in Year 10 and above emails and classwork will be retained for the current academic year and 1 year as these may include for coursework assessment, exam appeals etc.	SECURE DISPOSAL

Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 1 month for field file + 5 years for financial data + 25 years (Major events or safeguarding) Financial information related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions. A 'field file' is the information that is taken on a trip by a school. This can be destroyed	SECURE DISPOSAL

				following the trip, once any medicines administers on the trip have been entered onto the core system. If there is a minor medical incident on the trip (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school'), then adding it into the core system would be done. If there is a major incident (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate. Permission to go on the trip slips will contain personal data, and destroying them after the trip unless any significant incident arises is appropriate, otherwise refer to the policies above. Schools sometimes share personal data with people providing 'educational visits' into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.	
7.1.2	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.

7.1.3	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority.

8.1 Local Authority					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL

8.2 Central Government					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.2.1	ISI reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

9.0 Photographs					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
9.0.1	Photographs	No		Images are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent, captured at the outset of using the photograph. This is 10 years from the date the photograph was taken. Nb Please note, we will not use photographs when they are over 10 years old but they may still be accessible, for example, if a visitor retains a copy of the prospectus from a former visit or someone were to review historic posts on social media.	SECURE DISPOSAL

10.0 SARs

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
10.0.1	SAR	No		6 Years – copy of data given as well as redaction records	SECURE DISPOSAL