GDPR

DATA PROTECTION POLICY

Contents

DATA PROTECTION POLICY

Background

Data protection is an important legal compliance issue for Thornton College (the "School"). During the course of the School's activities we collect, store and process personal data (sometimes sensitive in nature) about staff, pupils, their parents, contractors and other third parties (in a manner more fully detailed in the our Privacy Notice). We, as the data "controller", are liable for the actions of our staff and trustees/directors/ 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 "UK 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 in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

Definitions

Key data protection terms used in this data protection policy are:

- **[Data] Controller** – 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 controller.
- **[Data] Processor** – an organisation that processes personal data on behalf of a 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.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **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.
- **Processing** – virtually anything done with personal data, 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.

- **Special categories of personal data –** 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.

Application of this policy

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

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.

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 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where we share personal data with third party controllers – which may range from other schools, to parents and appropriate authorities – 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.

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.

Person responsible for Data Protection at the School

We have appointed Jane Sanders (Bursar) as the Data Protection Co-ordinator who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Co-ordinator.

The Principles

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

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The UK GDPR's broader 'accountability' principle also requires that we not only process 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:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and
- 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.

Lawful grounds for data processing

Under the UK 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 the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable that we rely on another lawful ground where possible.

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 that we are taking on extra responsibility for considering and protecting people's rights and interests. Our legitimate interests are set out in its Privacy Notice, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- 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.

Headline responsibilities of all staff

Record-keeping

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

You 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 you from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is that you **record every document or email in a form you would be prepared to stand by should the person about whom it was recorded ask to see it**.

Data handling

You have a responsibility to handle the personal data which you 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 you). 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 you should read and comply with the following policies:

- Staff Handbook
- Safeguarding & child Protection
- IT and E-Safety
- Camera use policy (see Appendix 3)

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report

certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, we must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify Jane Sanders, Bursar. If you 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 we always need to know about them to make a decision.

As stated above, we 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.

Care and data security

More generally, we require you (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use your best efforts to comply with those principles whenever you 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 the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

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 we use personal information to Jane Sanders, Bursar, and to identity the need for (and implement) regular staff training. You must attend any training we require you to.

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:

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

The default school policy is to store assessment data on One Drive/MS Teams, iSams and SISRA 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.

Lock computers when not in use.

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.

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

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

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.

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

Not to email, fax or post data to others, even those within our organisation

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

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

Keep the staffroom door locked at all times

Regularly update passwords in line with the school IT policy, these should be appropriately complex and not disclosed to others under any circumstances

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

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.

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.

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.

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

If this is not possible, save it on One Drive as this is password protected, secured by two factor authentication and backed up.

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.

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. These are available from the medical centre, prior written consent from the Bursar must be attained; this approach is for exceptional circumstances only.

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.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to Jane Sanders, Bursar in the first instance, and at as early a stage as possible.

Rights of Individuals

In addition to responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a 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), you must tell Jane Sanders, Bursar as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- 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
- 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.

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

- 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).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell Jane Sanders, Bursar as soon as possible.

Data Security: online and digital

We 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.

- You are not permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
- You should not provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Use of personal email accounts, social media, SMS or personal devices by governors/trustees or staff for official School business is not permitted.

SUMMARY

"*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 our School's culture and all its staff and representatives need to be mindful of it.

Staff Privacy Notice: Please note that this can be found in the appendices of this document

DATA RETENTION

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.

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.

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

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.

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.

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.

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.

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

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.

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.

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

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.

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.

The Bursar should be informed of this request immediately.

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 unavailable, then staff should contact any member of the SLT.

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

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.

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

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.

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

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.

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.

Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the School can: charge a reasonable fee taking into account the administrative costs of providing the information; or refuse to respond.

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.

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

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.

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.

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 STAFF PRIVACY NOTICE

Who we are

We are Thornton College of Jesus and Mary (the "School") charity registration number 247358 with registered office is at Thornton College, Thornton, Milton Keynes, Buckinghamshire, MK17 0HJ.

In the course of your work undertaken for the School, we will collect, use and hold ("process") personal data relating to you as a member of our staff or wider school team, regardless of your employment status. This makes us a controller of your personal information, and this Privacy Notice sets out how we will use that information and what your rights are.

Who this notice applies to

This notice applies to staff at the School, including current, former and prospective: employees, self-employed contractors, visiting music teachers and other peripatetic workers, casual workers, temps, and volunteers who may be employed or engaged by the School to work for it in any capacity, as well as prospective applicants for roles. This also applies to governors / trustees / directors.

Please note that references to "employment", "staff" etc. in this Privacy Notice are not intended to imply or confer any employment rights on you if you are a contractor, non-employed worker, or job applicant.

About this Notice

This Privacy Notice explains how we processes your personal data and your rights in relation to the personal data we hold about you.

This Privacy Notice applies in addition to our other relevant terms and conditions and policies that may (depending on your role and status) apply to you, including[1]:

- any contract between you and the School, such as the terms and conditions of employment, and including the staff code of conduct and any applicable staff handbook;
- our CCTV and/or biometrics policy;
- our retention of records policy;
- our disciplinary, safeguarding, pastoral, anti-bullying, or health and safety policies, including as to how concerns, low-level concerns or incidents are reported or recorded (both by and about staff);
- our data protection policy; and
- our IT policies, including our Acceptable Use policy, Online Safety policy, Social Media policy, WiFi policy, Remote Working policy and Bring Your Own Device policy.

Please note that any contract you may have with the School will be relevant to how we process your data, in accordance with any relevant rights or obligations under that contract. However, this Staff Privacy Notice is the primary document by which we notify you about our processing of your personal data.

This Staff Privacy Notice also applies alongside any other information we may provide about particular uses of personal data, for example when collecting data via an online or paper form.

How we collect your information

Before you are employed or engaged by the School, we may collect your personal data in a number of ways, for example[2]:

- from the information you provide to us before making a job application;

- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, or when you complete a self-declaration, etc.;
- when you attend an interview; and
- from third parties, for example the Disclosure and Barring Service ("DBS") and referees (including your previous or current employers or school), or from third party websites (as part of online suitability checks for shortlisted candidates) or (if you are a contractor or a substitute) your own employer or agent, in order to verify details about you and/or your application to work for us.

During the course of your employment or engagement with us, we will collect data from or about you, including:

- when you provide or update your contact details;
- when you or another member of staff completes paperwork regarding your performance appraisals;
- in the course of fulfilling your employment (or equivalent) duties more generally, including by filling reports, note taking, or sending emails on school systems;
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

The types of information we collect

We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant)[3]:

- contact and communications information, including:
- your contact details (including email address(es), telephone numbers and postal address(es);
- contact details (through various means, as above) for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this Privacy Notice;
- records of communications and interactions we have had with you;
- biographical, educational and social information, including:
- your name, title, gender, nationality and date of birth;
- your marital status and details of any dependents you may have;
- your image and likeness, including as captured in photographs taken for work purposes;
- details of your education and references from your institutions of study;
- lifestyle information and social circumstances;
- your interests and extra-curricular activities;
- information in the public domain, including information you may have posted to social media, where relevant to your role (e.g. as part of pre-employment screening);
- financial information, including:
- your bank account number(s), name(s) and sort code(s) (used for paying your salary or invoices and processing other payments);
- your tax status (including residence status);
- Gift Aid declaration information, where relevant (for example, where we help you to administer donations to charity from your pre-taxed earnings);
- information related to pensions, national insurance, or employee benefit schemes;

- work related information, including:
- details of your work history and references from your previous employer(s);
- records of your work at the School (including your start date, working hours, training records and performance / appraisal records, and information about your use of our IT systems);
- your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for the school;

- if applicable, recordings of your lessons and other meetings with staff and pupils, and of your participation in School events;
- details of your professional activities and interests;
- your involvement with and membership of sector bodies and professional associations;
- information about your employment and professional life after leaving the school, where relevant (for example, where you have asked us to keep in touch with you);
- details of your right to enter, live and work in the UK, including your nationality and other immigration status information (ie about your entitlement to work in the UK), including copies of passport information (if applicable);
- details of any disciplinary matters or grievances which you raise or which relate to you;
- and any other information relevant to your employment or other engagement to work for the school.

Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data, and information about criminal convictions and offences, including:

- information revealing your racial or ethnic origin;
- trade union membership, where applicable;
- information concerning your health and medical conditions (for example, where required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment);
- information concerning your sexual life or orientation (for example, in the course of investigating complaints made by you or others, for example concerning discrimination); and
- information about certain criminal convictions (for example, where this is necessary for due diligence purposes, whether by self-declaration or otherwise, or for compliance with our legal and regulatory obligations).

However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for us.

The bases for processing your personal data, how that data is used and whom it is shared with

(i) ***Entering into, or fulfilling, our contract with you***

We process your personal data because it is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract, such as a contract of employment or other engagement with us. In this respect, depending on your role and status, we are likely to use your personal data for the following purposes:

- administering job applications and, where relevant, offering you a role with us;
- carrying out due diligence checks on you, whether during the application process for a role with us or during your engagement with us, including by checking references in relation to your education and your employment history and obtaining any required self-declarations;

- once you are employed or engaged by us in any capacity, for the performance of the contract of employment (or other agreement) between you and us;
- to pay you and to administer benefits (including pensions) in connection with your employment or other engagement with us;

- monitoring your attendance and your performance in your work, including in performance appraisals;
- monitoring your use of our IT systems to ensure compliance with our policies (including the School's IT Acceptable Use and E-Safety Policy);
- to assess and make decisions about your fitness to work, training and development requirements;
- to promote the School to prospective parents and others, including by publishing the work product(s) you create while employed by or otherwise engaged to work for the School;
- for disciplinary purposes, including conducting investigations where required;
- for other administrative purposes, for example to update you about changes to your terms and conditions of employment or engagement, or changes to your pension arrangements;
- for internal record-keeping, including the management of any staff feedback or complaints and incident reporting; and
- for any other reason or purpose set out in your employment or other contract with us.

(ii) ***Legitimate Interests***

We process your personal data because it is necessary for our (or sometimes a third party's) legitimate interests. Our "legitimate interests" include our interests in running the School in a professional, sustainable manner, in accordance with all relevant ethical, educational, charitable, legal and regulatory duties and requirements (whether or not connected directly to data protection law). In this respect, depending on your role and status, we are likely to use your personal data for the following:

- to provide you with information about us and what it is like to work for us (where you have asked for this, most obviously before you have made a formal application to work for us);
- for security purposes, including by operating security cameras in various locations on the School's premises[4];
- to enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- to provide education services to pupils, including where such services are provided remotely (either temporarily or permanently)[5];
- to safeguard staff and pupils' health and welfare and provide appropriate pastoral care;
- to carry out or cooperate with any school or external complaints, disciplinary or investigatory process;
- for the purposes of management planning and forecasting, research and statistical analysis;
- in connection with organising events and social engagements for staff;
- to make travel arrangements on your behalf, where required;
- to contact you or your family members and 'next of kin' for business continuity purposes, to confirm your absence from work, etc.;
- to publish your image and likeness in connection with your employment or engagement with us;
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT Acceptable Use and E-Safety Policy and government guidance such as KCSIE.

(iii) ***Legal Obligations***

We also process your personal data for our compliance with our legal obligations, notably those in connection with employment, charity / company law, tax law and accounting, and child welfare. In this respect, depending on your role and status, we are likely to use your personal data for the following:

- child welfare (including following the requirements and recommendations of KCSIE), social protection, diversity, equality, and gender pay gap monitoring, employment, immigration / visa sponsorship compliance and health and safety;
- for tax and accounting purposes, including transferring personal data to HM Revenue and Customs to ensure that you have paid appropriate amounts of tax, and in respect of any Gift Aid claims, where relevant;
- for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

(iv)***Special categories of data***

Depending on your role and status, we process special categories of personal data (such as data concerning health, religious beliefs, racial or ethnic origin, sexual orientation or union membership) or criminal convictions and allegations (treated for these purposes as special category data) for the reasons and purposes set out below.

In particular, we process the following types of special category personal data for the following reasons:

- your physical or mental health or condition(s) in order to record sick leave and take decisions about your fitness for work, or (in emergencies) act on any medical needs you may have;
- recording your racial or ethnic origin and sexual orientation in order to monitor our compliance with equal opportunities legislation;
- recording your trade union membership, in connection with your rights as an employee, agent or contractor and our obligations as an employer or engager of your services;
- to investigate complaints made by you or others, for example concerning discrimination, bullying or harassment, or as part of a complaint made against the School;
- data about any criminal convictions or offences committed by you, for example when conducting criminal background checks with the DBS, or via a self-declaration, or where a matter of public record (online or by any media), or where it is necessary to record or report an allegation (including to police or other authorities, with or without reference to you);

We will process special categories of personal data for lawful reasons only, including because[6]:

- you have given us your explicit consent to do so, but only in circumstances where seeking consent is appropriate;
- it is necessary to protect your or another person's vital interests, for example, where you have a life-threatening accident or illness in the workplace and we have to process your personal data in order to ensure you receive appropriate medical attention;
- it is necessary for the purposes of carrying out legal obligations and exercising legal rights (both yours and ours) in connection with your employment or engagement by us*;
- it is necessary in connection with some function in the substantial public interest, including:
- the safeguarding of children or vulnerable people*; or
- to prevent or detect unlawful acts*; or

- as part of a function designed to protect the public, pupils or parents from seriously improper conduct, malpractice, incompetence or unfitness in a role, or failures in services by the School (or to establish the truth of any such allegations)*; or
- or to cooperate with a relevant authority, professional or regulatory body (such as the ISI, DfE, LADO or TRA) in such matters*
- to comply with public health requirements (eg in respect of Covid-19 (or in similar circumstances)*; or
- it is necessary for the establishment, exercise or defence of legal claims, such as where any person has brought a claim or serious complaint against us or you.

(v) ***Low-level concerns about adults***[7]

We will process personal data about you, whether or not it constitutes special category data, in accordance with our policy on recording and sharing low-level concerns about adults (Please refer to the Safeguarding and Child Protection Policy). This will be processed for the same safeguarding and/or employment law reasons as set out above.

Such records are subject to the rules on retention set out in the our Safeguarding and Child Protection 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 7 years following the termination of your employment, but may need to be retained longer: e.g. where relevant, individually or cumulatively, to any employment, disciplinary or safeguarding matter. Low-level concerns will not be included in references unless they relate to issues which would normally be included in references, for example, misconduct or poor performance. A low-level concern which relates exclusively to safeguarding (and not to misconduct or poor performance) will not be referred to in a reference.[9]

Sharing your information with others

For the purposes referred to in this Privacy Notice and relying on the grounds for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases special category or criminal data) to a variety of recipients including:

- other employees, agents and contractors (e.g. third parties processing data on our behalf as part of administering payroll services, the provision of benefits including pensions, IT etc. – although this is not sharing your data in a legal sense, as these are considered data processors on our behalf);
- DBS and other **government authorities (e.g. HMRC, DfE, CAFCASS, police, Home Office, a relevant public health / NHS body and / or local authority) and/or appropriate regulatory bodies e.g. the Teaching Regulation Agency, the Independent Schools Inspectorate, the Charity Commission** etc.;
- third party background check agencies;
- external auditors or inspectors;
- our advisers where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, or other external consultants;
- third parties and their advisers in the unlikely event that those third parties are acquiring or considering acquiring all or part of the School, or we are reconstituting or setting up some form of joint working or partnership arrangement in the unlikely event that those third parties are acquiring or considering acquiring all or part of the School, or we are reconstituting or setting up some form of joint working or partnership

arrangement in the UK or abroad;

- when we are legally required to do so (by a court order, government body, law enforcement agency or other authority of competent jurisdiction), for example HM Revenue and Customs or police.

We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations. References given or received in confidence may not be accessible under your UK GDPR rights.

How long your information is kept[10]

Personal data relating to unsuccessful job applicants is deleted 6 months after the end of the application process, except where we have notified you we intend to keep it for longer (and you have not objected).

Subject to any other notices that we may provide to you, we may retain your personal data for a period of 7 years after your contract has expired or been terminated. However, some information may be retained for longer than this, for example incident reports and safeguarding files, in accordance with specific legal requirements. Please see appendix for further details of retention periods.

Your rights

Please see our External Privacy Notice which has details of your rights as a 'data subject', which are the same as if you were any member for the public.

This notice

We will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable. This Privacy Notice was lasted updated on the date specified in the footer of this document.

Contact and complaints

If you have any queries about this Privacy Notice or how we process your personal data, or if you wish to exercise any of your rights under applicable law, you may contact your line manager / refer the matter through the staff grievance procedure.

If you are not satisfied with how we are processing your personal data, or how we deal with your complaint, you can make a complaint to the Information Commissioner: www.ico.org.uk. The ICO does recommend you seek to resolve any issues with the data controller initially prior to any referral[11].

APPENDIX 3 : Retention periods

PP 66-67 OF UK GOVERNMENT DATA PROTECTION GUIDE FOR SCHOOLS. Plus Extracts from ISBA Retention of Records and Data. & 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 Admissions Process					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.4	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
1.3.7	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 Provision s	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 Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative 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	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 Provision s	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 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.	SECURE DISPOSAL

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

Appendix 4
Camera Use Policy v2.1

Introduction

Photographs and video for school and family use are a source of innocent pleasure and pride, which can enhance the self-esteem of students and young people and their families.

Parents/carers are not required to comply with the Data Protection Act 1998 when taking photographs for their own private use of their students at an organised event.

Parents should not be stopped taking photographs for their own private use because of concerns of contravening the Data Protection Act. However, we must always be mindful of the need to safeguard the welfare of students in our school, and issues of child protection, data protection and parental consent will be given careful thought. Images may be used to harm students, for example as a preliminary to 'grooming' or by displaying them inappropriately on the Internet.

This policy will apply to all forms of publications: print, film, video, DVD, on websites and in the professional media.

Where another body provides services or activities separately, using the school premises, the Bursar will ensure that the body concerned has appropriate policies and procedures in place in regard to safeguarding students.

Consent forms

1. All parents of students in the school will be asked to sign an online consent form to gain permission to publish photographs in public places (including websites). This form will include clear references to where the image may be used. If this list is added to, new permission MUST be sought. Parents will have the option of
    a. Full Consent (any purpose),
    b. Teaching, Learning and Official School Photographs only Consent (to record or aid teaching and learning or in formal form/year or whole class photographs)
    c. Teaching and Learning Consent (to record or aid teaching and learning)
    d. No Consent (not for any purpose).

    Even when No Consent is given, we have a legitimate interest to take photographs of the students for our internal use to enable staff to identify the student.

2. This consent will be sought when a child starts school; parents must be made aware that they can withdraw consent at any time and the mechanism to do this. Withdrawal of consent will be from the date the request is received by our administration team and will only apply to new publications after that date – it is not retrospective;
    i.e. we will attempt to identify and remove any photographs of the child already published, but in some cases this may not be possible.

3. A log is kept on School Post and on OneDrive of all parents/carer replies including the date and method by which consent was given. Where a parent proactively does not consent and failure to reply will both be treated as if consent has not been given and recorded on our log. If parents/carers disagree over consent for their child, it will be treated as if consent has not been given.

4. All adults in the school will be asked to sign a consent form to gain permission to publish photographs and moving images in public places (including websites) – this is part of their employment contact and managed by the Bursar.

Parents and carers

5. We do not allow parents/carers or attendees to take photographs and videos at school events as other students may inadvertently be captured. This includes, but not is limited to, smart watches, cameras, mobile phones or tablets. This will be clearly stated in the letter/ communications regarding events and a member of staff will announce this prior to events starting.
6. If general shots/footage are to take place such as at a school event, visitors will be warned in the invitation/communications. Tickets/reply slips and/or entry signage will include a warning that school photography/filming will take place at the event and ask visitors to select a lanyard on entering the event. If they choose no lanyard (proactive consent given to be in photographs) or yellow lanyard (do not consent to being in school photographs). The image(s)/ footage of the person will therefore show if the person has given consent and have a date of capture. Guests must be invited to make this choice when entering the event so they can make a pro-active opt-in choice under GDPR. Our school photographer will also wear a clear red high-vis vest that identifies their role and enables subjects to move away or request not to be photographed should they change their mind during the event.
7. People with no connection to our school will not be allowed to photograph – staff will question anyone they do not recognise who is using a camera and or video recorder at events and productions.

Creation of images

8. All photographs/footage must be taken on school cameras or school-owned iPads/devices. NO member of staff is permitted to take photographs on their own device (including, but not limited to, smart watches, cameras, mobile phones or tablets) for any purpose.

9. School iPads should be secured with a passcode which activates after 2 minutes without use. Staff should read and comply with the school ICT policy which states that school devices and their passcodes should not be shared with others, NB this includes students in school or friends/ family members outside of school.

10. Only image/ footage of students suitably dressed will be allowed to reduce the risk of images being used inappropriately. Special consideration will be given to photographs taken during PE (sports day), Dance and swimming.

11. No photographs or videos may be taken when students are dressing or changing.

12. No photographs or videos may be taken when students are receiving medical attention.

13. No photographs or videos should be taken in areas of the school where student data is held (unless a member of staff has previously checked that no data could be captured); this includes, but is not limited to, the staff room, administration offices, SEN Office and SEN Teaching Room, Bursary and Safeguarding Lead's Office.

14. If a photograph is likely to be used again it will be stored securely on the school network or OneDrive and MUST be deleted from the device upon which it was created. Images should only accessed by those people authorised to do so.

Students who should not be identified

15. Every effort will be made by the school to prevent capturing the image of any child who should not be identified.

16. The Marketing team will check online and print publications before they are published to ensure no images of children who should not be identified are included within the publication. The consent log will be used for this purpose.

Media photographing and filming

17. The media operate under their own Code of Practice. Photographs taken by the media are usually exempt from the Data Protection Act.

18. If the media are invited into school for publicity purposes parents/carers of those students likely to appear will be informed.

Video Conferencing and Web Cameras

19. Where parents have asked that their children's images should not be included in video conference or web camera every effort will be made to avoid this.

Mobile phones (MMS MultiMedia messaging service, video phones), Tablets and Smart Watches

20. Mobile phones, tablet devices and smart watches should not be used to capture or transmit images unless where it is linked to learning AND permission has been granted by the teacher (e.g. Capturing images/notes of board, videoing a practical). It is important that during such occurrences no other child is in the clip taken. Teacher will vet any photo where it is believed this has occurred. (SEE MOBILE PHONE POLICY)

CCTV

21. CCTV *(where installed)* will be operated in accordance with the principles of data protection.

See Information Commissioner Guidance which can be found at:
http://www.ico.gov.uk/documentUploads/cctvcop1.pdf. *Guidance for parents*

If at any time you wish to withdraw this consent, please contact sheap@thorntoncollege.com

A guide for parents who wish to use photography and/or video a school event

Parents/carers and others, attend school events at the invitation of the Headteacher and Community. The Headteacher and Community have the responsibility to decide if photography and videoing of a particular event is permitted. We do not allow parents/carers or attendees to take photographs or videos at school events as other students may inadvertently be captured.

Where we have consent, our school photographer will capture events and these images will be shared with parents and carers. Parents and carers can view these photographs and videos taken at a school event for their own personal use only. Such photographs and videos must not be downloaded, recorded or sold and must not be put on the web/internet, other than on official Thornton College channels. To do so would likely break Data Protection legislation.

Recording or photographing would require a written record of the date and method of the express, proactive consent of all persons captured. NB where the person is under thirteen years old this permission would need to be obtained from all persons with parental responsibility for that individual.

Parents and carers must not photograph or video students changing for performances or events.

If you are accompanied or represented by people that school staff do not recognise they may need to check who they are, if they are using a camera or video recorder.

Mobile devices (including, but not limited to, mobile phones, smart watches, cameras, mobile phones or tablets) should not be used to capture or transmit images.