
# GDPR

# DATA PROTECTION POLICY

# Contents

# DATA PROTECTION POLICY

## Background

Data protection is an important legal compliance issue for Thornton College (the "School / College"). During the course of the College's activities we collect, store and process personal data (sometimes sensitive in nature) about staff, students, 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 College (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 College'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, students, employees, contractors and third parties).

Those who handle personal data as employees or governors/trustees/directors of the College 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 College or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the College's personal data as contractors, whether they are acting as 'processors' on the College'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 Colleges 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 College

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles.

The School have taken the following steps to ensure and document UK GDPR compliance:-

**Data Protection Officer (DPO)**

Please find below details of the School's Data Protection Officer: -

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (option 1, then option 1 again)

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. Our Data Protection Advisors are Judicium Education, who are engaged to support the College and the Data Protection Co-ordinator. 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. Should the matter remain unresolved or require further escalation, please contact the school's DPO.

In particular, you can contact the DPO in the following circumstances:

a) If you are unsure of the lawful basis being relied on by the School to process personal data;

b) If you need to rely on consent as a lawful basis for processing (please see below the section on consent for further detail);

c) If you need to draft privacy notices or policies;

d) If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Retention Policy in the first instance];

e) If you are unsure about what security measures need to be put in place to protect personal data;

f) If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Breach Policy];

g) If you are unsure on what basis to transfer personal data outside the UK;

h) If you need any assistance dealing with any rights invoked by a data subject;

i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;

j) If you plan to undertake any activities involving automated processing or automated decision making;

k) If you need help complying with applicable law when carrying out direct marketing activities;

l) If you need help with any contracts, data processing agreements or other areas in relation to sharing personal data with third parties.

## 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.

## Training

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. The school will carry out adequate training with all staff annually.

## 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 College. 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 our relevant Privacy Notices, 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 College 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, students 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 College 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 students and parents, in accordance with the College'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 College's policies and procedures (to the extent applicable to you). In particular, there are data protection implications across a number of areas of the College's wider responsibilities such as safeguarding and IT security, so you should read and comply with the following policies:

- Staff Handbook
- Child Protection & Safeguarding
- IT Acceptable Use and E-Safety
- CCTV
- 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 Mrs 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 College, 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 affects 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 Mrs 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:

- ✓ Only access the personal data that you have authority to access, and only for authorised purposes;
- ✓ Only allow others to access personal data if they have appropriate authorisation;
- ✓ Keep all electronic records on a secure, password protected system such as the One Drive/MS Teams, iSams, SISRA, or CPOMS.
- ✓ The default College policy is to store assessment data on One Drive/MS Teams, iSams and SISRA as these are accessed via the College 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 College 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 College 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 College 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 College IT Acceptable Use & Online E-Safety 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 College IT equipment with other College 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 College.

***Marking:*** It may not be possible to mark all student work in College during the school day. Therefore, staff are permitted to take student work home to be assessed. 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 College 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 College'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 College). 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:

- request access to their personal data that we hold (see “Subject Access Requests” at Appendix 4);
- 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);
- receive certain information about the School’s processing activities;
- 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.
- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- challenge processing which has been justified on the basis of legitimate interests or in the public interest;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- To raise a concern or make a complaint directly to the School if they believe their personal data has been processed unlawfully or unfairly, or if they are dissatisfied with the School’s response to a data protection request. Individuals also have the right to make a complaint to the supervisory authority, which is the Information Commissioner in England and Wales (https://ico.org.uk/global/contact-us/).

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. If any request is made to exercise the rights above, it is a requirement to verify the identity of the individual making the request.

## Data Security: online and digital

The College 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.

- X No member of staff is permitted to remove personal data from College premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar.
- X No member of staff should provide personal data of students or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- X Use of personal email accounts or unencrypted personal devices by governors/trustees or staff for official College business is not permitted.

## Processing of Financial / Credit Card Data

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

## Audit

Thornton College regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data. An action plan is put into place for outstanding actions.

## 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 College will use the guidelines set out in the ISBA Guidelines for Independent Schools on the Storage and retention of Records. The data retention timelines are laid out in the appendices of this policy.

It is the duty of the College 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 College Bursary Finance 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 College administration team to delete other data such as pupil records 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 Head's PA to ensure staff records are appropriately in line with this policy. The Executive Team will review and agree staff safe files to be removed. [Files are archived at the start of each term.]

It is the duty of Head of Admissions to ensure prospective student records are maintained appropriately.

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 365 days, for most email accounts. 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 Requests

The GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them can be made verbally or in writing to any member of staff and will be handled in Accordance with our '**Subject Access Request Procedures**' at Appendix 5 of this policy. A request form is available at Appendix 6.

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 College 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 College 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 College's decision (to comply or refuse the request) within 28 days. NB this includes weekends and holiday periods. The College aims to make the data available within one month of the request, the College may take a further two months to complete an SAR that is complex.

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 College 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 College 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 students 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 student (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 students may be considered mature enough to exercise their own subject access rights]. In every case it will be for the College, 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 students 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 student 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 College consider the child to be mature enough to understand their rights under the GDPR, the College shall ask the student 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 College to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the College 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 College'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 College 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 College 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.

## Data Subject Complaints

Individuals have the right to make a complaint directly to us if they believe their data protection rights have been breached.

We will acknowledge receipt within 30 days and provide a substantive response without undue delay. If you are not satisfied with our response, you may escalate the matter to the Information Commissioner's Office (ICO).

Further information about how the Trust handles data protection complaints can be found at Appendix 7 of this policy, along with a data protection complaints form at Appendix 8. Complaints must be made in writing to Mrs Jane Sanders, Bursar at bursar@thorntoncollege.com.

## Personal Data Breaches

The UK GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so. Please refer to our Data Breach Response Policy & Procedures found at Appendix 9 of this policy document below.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches who is Mrs Jane Sanders or the School's DPO.

## Data Protection Impact Assessments (DPIAS)

In order to achieve a privacy by design approach, the School conduct DPIAs for any new high-risk technologies or programmes being used by the School which could affect the processing of personal data. The School carries out DPIAs when required by the UK GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data; and
- For large scale, systematic monitoring of a publicly accessible area (for example, through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- Details of what types of data are shared;
- Steps taken by the third party and the school in order to protect data;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

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

## Privacy Notices:

These include:

Data Privacy Notice – Students & Parents [including old Thorntonians] – available on our website

Visitors' Data Privacy Notice – available on our website

Staff Data Privacy Notice – available on the All Staff Sharepoint

Governors & Trustees Privacy Notice – within the Governors Handbook

# 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: Data Retention periods

This section contains retention periods connected to the College. [All secure disposal should be taken to mean disposal using a cross cut shredder, to include collection by a third party shredding company.]

| Type of Record/Document | Suggested Retention Period |
|---|---|
| **EMAILS & USER ACCOUNTS ON SERVER** | |
| Student email & user accounts | Accounts are disabled when a student leaves the school, which happens automatically through the Salamander software.<br><br>From pre-reception to year 9 when leaving, we keep their accounts disabled for a period of 3 months, upon which they are deleted. This includes emails. Routine automatic deletion of historic emails after 90 days on a rolling basis.<br><br>Years 10-13 we keep the accounts disabled for a period of 1 year just in case coursework is required etc. After 1-year accounts are deleted. Routine automatic deletion of historic emails after 1 year on a rolling basis. |
| Staff email & user accounts | Routine automatic deletion of historic emails after 1 year for the majority of staff. [A handful of staff are not included in this – such as Head, Bursar & Finance Manager.]<br><br>Accounts are automatically disabled when a member of staff leaves the school; through the Salamander software.<br><br>Accounts are disabled for a period of 1 year just in case information is required. After 1 year accounts are deleted; unless a senior staff member or administrator requires otherwise. |
| **INDIVIDUAL PUPIL RECORDS** - ***these records will contain personal data*** | |
| Enquiry Records [on iSams] | 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. |
| Applicant Records [on iSams] | All data for prospective students who have paid a registration fee are stored in digital form within iSams Applicant Database. These records will be reviewed annually and active applicants will remain until such time as the parents indicate that they no longer wish to be on our database. Those students who have had places declined will be removed after 1 year. |
| Admissions: application forms, assessments, parent contract, records of decisions | 25 years from date of birth (or up to 7 years from the pupil leaving). If unsuccessful: up to 1 year. |
| Student immigration records – UKVI Sponsorship etc | Duration of student sponsorship plus min. 1 year |
| Examination results (external or internal) | 7 years from pupil leaving school - in line with student record above. |

| | |
|---|---|
| Student file including:<br>• Pupil reports and performance records<br>• Pupil medical records (*not accidents*)<br>• Behaviour & Exclusions | 25 years from date of birth |
| Special educational needs records | Date of birth plus up to 35 years (*risk assessed*) |
| **SAFEGUARDING – *refer to IICSA guidelines*** | |
| Policies, procedures and insurance | Keep a permanent record of historic policies |
| Child Protection files and specific records of child sexual abuse | If a referral has been made / social care have been involved / child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years. |
| Video recordings of meetings | Where any one-on-one meetings of classes, counselling, or application interviews are recorded (e.g. for safeguarding purposes), a shorter-term retention policy is acceptable based on the DSL's view of how quickly a concern will likely be raised: e.g. 3-6 months or immediately upon DSL review. |
| DBS disclosure certificates | No longer than 6 months from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on SCR / personnel file, but not the certificate itself. |
| Accident / Incident reporting | 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. |
| **EMPLOYEE / PERSONNEL RECORDS - *these records will contain personal data*** | |
| Single Central Record of employees | Keep a permanent record that mandatory checks have been undertaken (but do not keep DBS certificate information itself: 6 months as above) |
| Job application and interview records (successful applicants) | Duration of employment plus minimum of 7 years |
| Job application and interview/rejection records (unsuccessful applicants) | 12 Months |
| Contracts of employment | 7 years from effective date of end of contract |
| Employee appraisals or reviews | Duration of employment plus minimum of 7 years |
| Staff personnel file | Duration of employment plus minimum of 7 years but do not delete any information which may be relevant to historic safeguarding claims. |
| Agency staff | Duration of employment plus minimum of 7 years but do not delete any information which may be relevant to historic safeguarding claims. |
| Allegation of a child protection nature against a member of staff including where the allegation is unfounded | Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer than REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found to be true, they are to be kept on the file and a copy provided to the person concerned |

| | |
|---|---|
| Disciplinary Proceedings:<br>• oral warning<br>• written warning – level 1<br>• written warning – level 2<br>• final warning | <br>• Date of warning + 6 months<br>• Date of warning + 6 months<br>• Date of warning + 12 months<br>• Date of warning + 18 months |
| Records of low-level concerns about adults | At least until end of employment (as recommended by KCSIE), then subject to review for relevance: e.g. 7 years from end of employment if they have ongoing relevance for employment claims, longer if necessary for safeguarding purposes / claims. |
| DBS disclosure certificates | No longer than 6 months from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on SCR / personnel file, but not the certificate itself. |
| Staff immigration records (Right to work, etc.) & Tier 2 migrant worker sponsor records | Minimum – 2 years from end of employment |
| Health records relating to employees | 7 years from end of employment |
| iSAMS | Records of dates employed to be kept. All documents attached containing personal data to be removed as outline above. |
| **SCHOOL-SPECIFIC RECORDS** | |
| Registration documents of School | Permanent (or until closure of the school) |
| Attendance Register | 6 years from last date of entry, then archive. |
| Detail on authorised absence | Up to one year |
| Departmental Curriculum Planning | 2 years |
| Marks/Timetables and Assignments | Current academic Year + 1 year |
| Minutes of Executive & SLT Meetings | 7 years |
| Staff Briefing Minutes | 3 years |
| General Correspondence | 7 Years |
| School Development Plan | Life of the plan + 7 years [previous SDP] |
| Policies [excludes CP & Safeguarding & H&S] | Life of Policy + 3 years |
| CP, Safeguarding and Health and Safety Policies | Permanent record |
| School census returns | Current Academic Year plus 5 previous school years. |
| ISI/Diocesan Reports | Life of report plus 2 previous reports (unless within Governors minutes) |
| Photographs | Students are photographed for marketing purposes [with parental permission] and we will not use photographs or footage taken 10 years or more. |
| Photographs and Footage | Photos and footage will be retained for archive purposes and kept indefinitely. |

| | |
|---|---|
| **GOVERNING BODY RECORDS** | |
| Trust Deeds | Permanent (or until dissolution of the company) |
| Minutes, Papers, Reports and Resolutions of Boards or Committee Meetings | Minimum – 10 years |
| Annual reports | Minimum – 10 years |
| **ACCOUNTING RECORDS** | |
| Accounting records | Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place. This means the current financial year plus 6 previous years.<br>Year End Financial Accounts kept in Bursar's office indefinitely. |
| Billing extras & WAC registers | Minimum 3 years-7 years |
| Tax returns | Up to 7 Years |
| VAT returns | Up to 7 Years |
| Budget and internal financial reports | Up to 7 Years |
| Payroll, salary, maternity pay records | Up to 7 Years [See pension exception below] |
| Pension or other benefit schedule records | Potentially permanent (ie lifetimes of those involved), depending on nature of scheme. |
| **CONTRACTS AND AGREEMENTS** | |
| Signed or final/concluded agreements, to include leases (*plus any signed or final/concluded variations or amendments*) | Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later |
| Deeds (or contracts under seal) | Minimum – 13 years from completion of contractual obligation or term of agreement |
| IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents) | Minimum – 7 years from completion of contractual obligation concerned or term of agreement |
| **INSURANCE RECORDS** | |
| Insurance policies (private, public, professional indemnity, cyber etc) | 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. |
| Employers Liability Insurance | Closure of School + 40 years |
| Correspondence related to claims/ renewals/ notification re: insurance | Minimum – 7 years (*but this will depend on what the policy covers and whether e.g. historic claims may still be made.* |
| **ENVIRONMENTAL, HEALTH, SAFETY & DATA** | |
| Maintenance logs | 10 years from date of last entry |

| | |
|---|---|
| Accidents to children & RIDDOR reports | 25 years from birth (longer for safeguarding) [Be aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. Therefore, keep a note of all procedures as they were at the time, plus a record that they were followed, and relevant insurance documents.] |
| Accident at work records (staff) | Minimum – 7 years from date of accident, but review case-by-case where possible taking reference to the note made above. Consider if the RA needs to be saved for longer. |
| Staff use of hazardous substances COSHH | Minimum – 7 years from end of date of use [Asbestos 40 years] |
| Covid-19 risk assessments, consents etc. (*for now: this to be subject to further review*) | Retain for 7 years legal paperwork (consents, notices, risk assessments) but not individual test results |
| Risk assessments (carried out in respect of above) | 7 years from completion of relevant project, incident, event or activity. |
| Art.30 UK GDPR records of processing activity (**ROPAs**), data breach records, data protection impact assessments | No limit (as long as no personal data held), but must be kept up-to-date, accurate and relevant. |
| SARs | 7 years – copy of data as well as redaction records |

# Appendix 3: Camera Use Policy v3

**Introduction**

Photographs and video for College 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.

These include but are not limited to:

- Teaching and Learning
- Official School Photographs
- Extra-Curricular Activities
- Celebrations & School Productions
- Marketing – Including Social Media

Photographs and video recordings of students constitute **personal data under UK GDPR**, and the College is committed to ensuring that all imagery is processed lawfully, fairly, transparently and securely.

Parents/carers are not required to comply with the Data Protection Act 1998 when taking photographs for their own private use of their children 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, the College must always prioritise **safeguarding, data protection and consent**, recognising that images may be misused, including being copied, altered, or manipulated using emerging technologies such as artificial intelligence.

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

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

**Key Principles (GDPR and Safeguarding)**

The College adopts a **safeguarding-first and data minimisation approach** to the use of images:

- Images will only be used where there is a **clear and legitimate purpose**
- The **least identifiable images** will be used wherever possible
- The risks of **online misuse, image scraping and AI manipulation** will be actively mitigated
- Personal data will not be retained longer than necessary

***Consent forms***

1. All parents of students in the College 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** – parents give permission for photographs, recordings, and video of their daughter to be taken and used by the school in the ways outlined above for teaching and learning, official school photographs, extra-curricular activities, celebrations & school productions and marketing including social media.

B) **No Consent** – parents do not give permission for photographs, recordings, and video of their daughter to be used by the school other than for essential reasons including but not limited to identification.
C) **No Consent Except For Official School Photographs** – as above but with the exception of traditional school class photographs and the whole school photograph

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 of all parents/carer replies including the date and method by which consent was given and then the permission is transferred to student files within isams. 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 College 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 contract.

**Parents and carers**

5. We allow parents/carers or attendees to take photographs and videos at College events of their own children as long asother students are not captured. This includes, but not is limited to, smart watches, cameras, mobile phones or tablets. A member of staff will announce this prior to events starting.
6. If general shots/footage are to take place such as at a College event, visitors will be warned in the invitation/communications. Tickets/reply slips and/or entry signage will include a warning that College 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 College 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 College 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 College 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 College cameras or College-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. College iPads should be secured with a passcode which activates after 2 minutes without use. Staff should read and comply with the College IT Acceptable Use & Online E-safety policy which states that College devices and their passcodes should not be shared with others, NB this includes students in school or friends/ family members outside of school.
10. 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.

***Image Content & Data MInimisation***

11. The College will ensure that:
    - Students are **not unnecessarily identifiable**
    - Full names, badges or identifying details are avoided
    - Group images or non-direct shots are used where possible
12. 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.
13. No photographs or videos may be taken when students are dressing or changing.
14. No photographs or videos may be taken when students are receiving medical attention.
15. 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.

***Image Security and AI Risk Mitigation***

The College recognises increasing risks associated with **image misuse and AI-based manipulation**, including copying, editing or generating harmful derivative content. This is risk assessed at Appendix 10.

16. To mitigate these risks, the College will:

    - Remove metadata (e.g. location and device data) before publication
    - Use **lower resolution or less detailed images** where appropriate
    - Limit images shared on publicly accessible platforms
    - Apply **privacy settings and restricted access controls**
    - Consider protective measures such as watermarking or secure platforms
    - Avoid publishing images that could reveal routines, locations or identifiable patterns

17. These measures are designed to reduce the risk of:

    - Unauthorised image reuse or "scraping"
    - Safeguarding harm or exploitation
    - Blackmail or manipulation of images
    - Reputational damage to individuals or the College

***Students who should not be identified***

18. Every effort will be made by the College to prevent capturing the image of any child who should not be identified.
19. 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 in iSams will be used for this purpose.

***Staff Responsibilities and Training***

20. All staff must:

    - Follow this policy and associated safeguarding guidance
    - Check images before use for identifiable information
    - Report concerns or breaches immediately

21. The College will provide **regular training** covering:

- GDPR and data protection
- Safe use of images
- Risks associated with AI and online misuse

***Media photographing and filming***

22. The media operate under their own Code of Practice. Photographs taken by the media are usually exempt from the Data Protection Act.
23. If the media are invited into College for publicity purposes parents/carers of those students likely to appear will be informed.

***Video Conferencing and Web Cameras***

24. 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***

***25.*** 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***

26. CCTV (*where installed*) will be operated in accordance with the principles of data protection and is covered by our CCTV Policy.

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

***Incident Response (Misuse, Breach or AI Manipulation)***

27. In the event of misuse or unauthorised use of images, the College will:

    - Remove images where possible
    - Notify the Designated Safeguarding Lead
    - Record and assess the incident
    - Follow data breach reporting procedures

28. Where appropriate:

    - Incidents may be reported to the police or relevant authorities
    - Safeguarding support will be provided to affected individuals

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

Parents/carers and others, attend College 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 College events as other students may inadvertently be captured.

Where we have consent, our College 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 College 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 College 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.

**Related Policies**

This policy should be read alongside:

- Safeguarding Policy
- Online Safety Policy
- IT Acceptable Use Policy
- CCTV Policy

## Appendix 4: Subject Access Request (SAR) Procedure

1. What is a Subject Access Request?Under the UK GDPR and the Data Protection Act 2018, individuals have the right to request access to the personal data the School holds about them.

A valid SAR may be made verbally or in writing, to any member of staff, and does not need to mention "subject access" or the legislation.

Staff must treat any request to access personal data as a SAR and pass it immediately to the Data Protection Lead / DPO.

---

2. Recognising a SAR

A SAR may include statements such as:

- "Please send me all the information you hold about me"
- "I'd like to see my child's records"
- "What data do you have about me?"

A SAR may be made via:

- Email
- Letter
- Telephone call
- In person
- Messaging or digital platforms (eg. Social media)

Any staff member receiving such a request must forward it on the same day.

---

3. Acknowledging a SAR

The School will:

- Acknowledge the SAR within one calendar month;
- Request ID verification where needed;
- Request clarification if the request is broad or unclear (the one-month period may be paused until clarification is received);
- Inform the requester of the expected timeframe.

Where a request is received during a school holiday, acknowledgement may be delayed until the School reopens, and this will be communicated to the requester where possible

---

4. Verifying Identity

Before responding, the School will take reasonable steps to confirm the requester's identity. Acceptable documents include:

- passport
- driving licence
- birth certificate
- recent utility bill or official letter showing name and address

Where a request is made by a third party (e.g., solicitor or parent acting for a child), evidence of authority to act must also be provided.

---

5. Timeframe for Response

The School must respond within one calendar month from:

- the date of receipt, or
- the date sufficient ID is received, or
- the date clarification is provided, or
- the date any applicable fee is paid (in rare cases)

For complex or large-scale requests, the response may be extended by up to two further months. The School will inform the requester of any extension within the initial one-month period.

---

6. Locating the Information

A coordinated search may include:

- emails and digital correspondence
- MIS systems (e.g., ISAMS,)
- safeguarding systems (e.g., CPOMS,)
- HR and payroll systems
- paper files and manual records
- assessments, reports and meeting minutes
- CCTV footage (subject to exemptions)
- data held by third-party processors

Searches must be reasonable and proportionate based on the request.

---

7. Third-Party Data and Redaction

The School must not release information identifying another individual unless:

- the individual has given consent, or
- it is reasonable to disclose without consent

Where possible, information will be redacted to protect third-party identities.

---

8. Exemptions

Certain information may be withheld where permitted under law, including:

- references (given or received)
- information relating to crime prevention/detection
- legal professional privilege
- management forecasting or negotiations that would be prejudiced by disclosure
- data containing confidential third-party information that cannot be redacted

Any use of exemptions must be carefully assessed and documented.

---

9. Format of the Response

The School will provide:

- a copy of the personal data requested
- supplementary information required under Article 15 UK GDPR
- clear explanations in plain language

Where the SAR is submitted electronically, the response will normally be provided in a commonly used electronic format (e.g., PDF), unless the requester asks otherwise.

---

10. Record Keeping

The School will keep a log of:

- the date the SAR was received
- the requester's name
- the nature of the request
- actions taken during the search
- the date of the final response
- whether any exemptions were applied

Records will be kept in accordance with the School's Retention Schedule.

## Appendix 5: Subject Access Request Form

(Use of this form is optional. Individuals may submit a SAR in any format.)

---

Section 1 – Details of the Data Subject

| Information | Detail |
|---|---|
| Title: | |
| Full Name: | |
| Date of Birth: | |
| Address: | |
| Postcode: | |
| Phone Number: | |
| Email Address: | |

Proof of Identity enclosed (please tick one):

☐ Passport

☐ Driving licence

☐ Birth certificate

☐ Recent utility bill / official letter

---

Section 2 – Details of the Request

Please describe the information you are requesting. Include any relevant dates, departments, names, or contexts to assist the School in locating the data:

Details of the request:

| |
|---|
| |

If your request relates to employment records, please provide:

| | |
|---|---|
| **Job title** | |
| **Employment dates** | |
| **Department/line manager (if known)** | |

---

Section 3 – Requester Acting on Behalf of the Data Subject (if applicable)

| | |
|---|---|
| Your Name: | |
| Relationship to Data Subject: | |
| Address: | |
| Email: | |
| Phone: | |

Proof of identity enclosed for requester (tick one):

☐ Passport

☐ Driving licence

☐ Birth certificate

☐ Recent utility bill

Proof of authority to act (tick one):

☐ Letter of authority

☐ Power of Attorney

☐ Evidence of parental responsibility

☐ Other (please specify):

---

Section 4 – Preferred Method of Receiving Information

☐ Email

☐ Post*

☐ Collection in person

☐ View only

☐ Review with a member of staff

*If choosing postal delivery, please note that although the School takes care when sending information, it cannot be held liable for loss or misdelivery.

---

Section 5 – Declaration

I confirm that the information provided in this form is accurate and that I am the data subject or legally authorised to act on behalf of the data subject.

Signature:……

Date:……

Please return this form and proof of identity to:
Mrs Jane Sanders, Bursar - Data Protection Lead on bursar@thorntoncollege.com

# Appendix 6: Data Protection Complaints Procedure

1. Purpose of this Procedure

This procedure explains how individuals may raise concerns or make complaints about how Thornton College processes personal data, and how the School will respond. It ensures that data protection complaints are handled promptly, lawfully and fairly, in line with the UK GDPR and the Data (Use and Access) Act 2025.

A data protection complaint is any expression of dissatisfaction about the School's handling of personal data, including:

- concerns about inaccuracy, inappropriate use, or excessive data
- delays or failures in responding to data subject rights requests (e.g., SARs)
- concerns about a potential personal data breach
- concerns about transparency or fairness in data processing
- concerns about automated decision-making or profiling

A complaint does not need to reference "data protection", "privacy", or "UK GDPR" to be valid.

---

2. Who Can Make a Complaint

Any individual, or a representative acting on their behalf, may make a data protection complaint. This includes:

- parents
- pupils (where age-appropriate)
- current or former staff
- volunteers
- contractors
- any person whose data the School processes

Where a representative makes a complaint, the School may request evidence of authority to act.

---

3. How to Make a Complaint

Complaints can be made:

- in writing (email or letter)
- verbally (in person or by telephone)
- using the Data Protection Complaints Form (Appendix 8)

Complaints should be directed to: Mrs Jane Sanders, Bursar on Email: bursar@thorntoncollege.com

If a complaint is received by any staff member, it must be forwarded immediately to the Data Protection Lead.

---

4. Acknowledging a Complaint

The School will:

- acknowledge the complaint within 30 calendar days
- provide the name and contact details of the person handling the complaint
- request any further clarification or evidence needed to investigate fully

Where further information is required, the investigation timeframe may be paused until it is received.

During school closure periods, acknowledgement may be delayed until the School reopens, and this will be made clear via an automatic response where possible.

---

5. Investigating a Complaint

The School will:

- investigate promptly, proportionately and impartially
- review relevant documents, systems or correspondence
- consult relevant staff or departments as needed
- involve the Data Protection Officer (DPO) where appropriate
- keep the complainant updated where possible

Investigations will be carried out confidentially and with due regard for the privacy of all individuals involved.

---

6. Outcome of a Complaint

The School will provide a written response setting out:

- whether the complaint is upheld, partially upheld or not upheld
- findings of the investigation
- any action the School will take to correct or prevent issues (if applicable)
- information on the right to escalate the matter to the Information Commissioner's Office (ICO)

A response will be provided without undue delay following completion of the investigation.

---

7. If the Complainant Remains Dissatisfied

Individuals who remain dissatisfied after receiving the School's response may escalate their complaint to the Headteacher, who will conduct an investigation in line with our Complaints Policy.

Information Commissioner's Office (ICO)
Website: https://ico.org.uk
Helpline: 0303 123 1113

The School will include ICO contact details in the written outcome.

---

8. Complaints Received During School Closure Periods

Where complaints are received during extended closure periods (e.g., school holidays), the School will:

- record the date of receipt
- acknowledge the complaint as soon as reasonably possible
- begin investigation promptly once the School reopens

Complainants seeking urgent resolution are encouraged to submit complaints during term time.

---

9. Record Keeping

The School will retain a record of:

- the date the complaint was received
- the complainant's name
- the nature of the complaint
- key steps taken during the investigation
- the outcome and date of response
- any follow-up actions

Records will be kept in accordance with the School's Retention Schedule.

## Appendix 7: Data Protection Complaints Form

*(Completion of this form is optional. Complaints may be raised in any format.)*

---

Section 1 – Complainant Details

| | |
|---|---|
| Title: | |
| Full Name: | |
| Date of Birth (if relevant): | |
| Address: | |
| Postcode: | |
| Phone Number: | |
| Email Address: | |

---

Section 2 – Details of the Complaint

Please describe your concern in as much detail as possible. Include dates, correspondence, names of departments involved, and any supporting information.

Description of the complaint:

| |
|---|
| |

Have you previously raised this concern with the School? ☐ Yes ☐ No

| | |
|---|---|
| If yes, please specify to whom and when: | |
| What outcome are you seeking? | |

---

Section 3 – Representative (if applicable)

If you are making this complaint on behalf of someone else, please complete the details below.

| | |
|---|---|
| Your Name: | |
| Relationship to Data Subject: | |
| Address: | |
| Email: | |
| Phone: | |

Proof of your identity enclosed (tick one):

☐ Passport ☐ Driving licence ☐ Official letter

Proof of authority to act (tick one):

☐ Letter of authority

☐ Power of Attorney

☐ Evidence of parental responsibility

☐ Other (please specify):

---

Section 4 – Declaration

☐ I confirm that the information provided in this form is accurate and that I am the data subject or legally authorised to act on their behalf.

☐ I understand that the School may need to verify my identity.

Signature:……

Date:……..

Please send your completed form to:

Mrs Jane Sanders, Bursar on bursar@thorntoncollege.com

# Appendix 8:Data Breach Response Policy & Procedures

1. Policy Statement

This policy sets out the procedures Thornton College must follow in the event of a personal data breach, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Personal data breaches can adversely impact individuals' rights and freedoms and, where required, must be reported to the Information Commissioner's Office (ICO) within 72 hours.

Thornton College is committed to ensuring robust breach detection, investigation, reporting, and documentation processes. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

---

2. Scope

This policy applies to:

- All staff (teaching and non-teaching)
- Governors or trustees
- Contractors, volunteers, and temporary workers
- Anyone handling School personal data in any form

It applies to personal data breaches involving electronic, paper-based, or any other form of data.

---

3. Definitions

3.1 Personal Data Breach

A personal data breach is any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Examples include:

- Sending personal data to the wrong recipient
- Loss or theft of a device containing data
- Unauthorised access by a third party
- Alteration of data without permission
- Loss of availability of essential data systems

Staff must be trained to recognise incidents and escalate them promptly.

---

4. Roles and Responsibilities

4.1 Governing Body

Ensures the School complies with its data protection obligations.

4.2 Data Protection Lead in consultation with DPO

Responsible for:

- Managing data breach investigations
- Advising on risk and corrective actions
- Determining whether the breach must be reported to the ICO
- Advising on notification to affected individuals

The breach should be reported to the designated Judicium team without delay.

4.3 All Staff

All staff must:

- Report any suspected breach immediately to Mrs Jane Sanders
- Escalate incidents using the School's internal breach reporting process
- Support containment and recovery efforts

Failure to follow procedure may result in disciplinary action.

---

5. Breach Response Procedure

5.1 Step 1: Identify and Report

- Any member of staff who becomes aware of a suspected breach must:
- Report it immediately to Mrs Jane Sanders
- Provide all known details (time discovered, data involved, individuals affected).

Prompt reporting is essential to meet the ICO's 72-hour deadline.

---

5.2 Step 2: Contain and Recover

Initial containment actions may include:

- Attempting to recall mis-sent emails
- Retrieving physical documents
- Locking or wiping lost devices remotely
- Preventing further unauthorised access https://www.gov.uk/guidance/data-protection-in-schools/managing-breaches-of-data

Immediate actions help reduce risk and potential harm.

5.3 Step 3: Investigate

The Bursar will conduct a formal investigation to determine:

- What happened and the cause
- Categories and volume of personal data involved
- Number and types of individuals affected
- Whether the data can be recovered

---

5.4 Step 4: Assess the Risk

A structured risk assessment will consider:

- Sensitivity of the data (including special category data)
- Likelihood and severity of harm
- Whether the breach poses a risk or high risk to individuals

This assessment determines whether notifications are required.

---

5.5 Step 5: Record the Incident

All breaches must be documented in the School's Data Breach Log, including:

- Incident details
- Risk analysis
- Actions taken
- Decision on ICO reporting [Judicium may be involved in this process]

Keeping a full record is a legal requirement, even where no report is made. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

---

5.6 Step 6: Notification to the ICO (If Required)

The School must notify the ICO within 72 hours if the breach is likely to pose a risk to individuals' rights and freedoms.

Notification must include:

- Nature of the breach
- Contacts and DPO details
- Likely consequences
- Measures taken or proposed

Partial information is acceptable initially, with updates provided later.

---

5.7 Step 7: Notification to Affected Individuals (If Required)

If the breach presents a high risk, individuals must be informed without undue delay.

The notification must:

- Describe the breach
- Outline likely consequences
- Provide advice on protective steps to take
- Detail actions being taken by the School

---

5.8 Step 8: Remedial and Preventive Actions

- Following containment and notification, the School will:
- Address vulnerabilities in systems or processes
- Provide additional staff training
- Update relevant policies and procedures
- Implement technical improvements if required

---

5.9 Step 9: Post-Incident Review

The DPO will conduct a formal review to determine:

- Root causes
- Lessons learned
- Effectiveness of the response
- Whether additional safeguards or training are needed

A report may be shared with senior leadership and governors.

---

6. Policy Review

This policy should be reviewed annually or:

- After any significant breach
- After changes in ICO guidance

- Upon updates to data protection legislation https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/toolkits/personal-data-breach-management/policies-and-procedures/

---

7. Associated Documents

- Data Protection Policy
- Staff Training Records
- Data Breach Log
- Incident Reporting Forms
- ICT Acceptable Use & E-Safety Policy & Cyber Security Strategy

---

Summary Checklist for Independent Schools

- ☑ Staff trained to recognise and report breaches
- ☑ Clear internal breach reporting policy
- ☑ Immediate containment actions
- ☑ Thorough investigation and risk assessment
- ☑ Accurate breach log
- ☑ ICO notified within 72 hours where required
- ☑ Affected individuals informed where high risk
- ☑ Remedial actions taken and reviewed
- ☑ Regular policy and training updates

---

# Appendix 9: Risk Assessment for School Use of Images

| Risk Area | Hazard Description | Who is at Risk | Potential Impact | Control Measures | Residual Risk |
|---|---|---|---|---|---|
| Misuse of Images | Images copied, altered or AI-manipulated once published online | Students, families, school | Safeguarding harm, distress, reputational damage | Increase use of non-identifiable images (side profile, back, taken from a distance, blurred images, over the shoulder, action shots, limit details of name, low resolution); Remove access to Flickr; Secure platforms where relevant; Remove metadata; Be more intentional with images | Medium |
| Consent | Images used without valid or informed parental consent | Students, families, school | GDPR breach, complaints, loss of trust | Written consent recorded; reviewed regularly (every September); clear explanation of image use; Senior students asked in-person on each occasion | Low |
| Identifiable Information | Names, badges or location data visible in images | Students | Increased vulnerability and targeting | Check images carefully; avoid full names; strip metadata before use | Low |
| Storage & Sharing | Images stored or shared on unauthorised or personal devices | Students and staff | Data breach, loss of image control | School-approved systems only; password-protected access; no personal accounts; audit and take appropriate action on front facing images especially | Low–Medium |
| Staff Awareness | Inconsistent understanding of acceptable image practice | Whole school community | Increased safeguarding risk | Clear policy; regular training; safeguarding reminders | Low |

**Date:** 11 May 2026

**Attendance:** LSW; TWS; SBL; JSS; MEX

**Updated:** August 2026