DATA PROTECTION FOR STAFF

BACKGROUND

Tonbridge School (a charitable company limited by guarantee, company number 4787097, registered charity number 1097977) is the data controller referred to in this policy as "the School". The School operates two schools: Tonbridge School and The New Beacon in Sevenoaks. The New Beacon is not a separate legal entity or a separate data controller. This policy applies in full at both schools, and references to the School include The New Beacon unless stated otherwise. Where the age of pupils requires a different operational position, in particular in the Nursery and Early Years, that difference is set out in The New Beacon Annex to this policy.

Data protection is an important legal compliance issue for the School. During the course of the School's activities, it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's General Privacy Notice). The School, as "data controller", is liable for the actions of its staff and 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.

The law that applies to the School is the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025. The 2025 Act made a number of changes which took effect in stages during 2026, including to automated decision-making, subject access and the handling of complaints. The DPA 2018 contains provisions of particular relevance to independent schools, notably in the context of our safeguarding obligations and the right of access to personal data. In this policy, "Data Protection Law" means the UK GDPR and the DPA 2018 as amended from time to time. The Information Commissioner's Office (ICO) enforces data protection law and has various powers to take action for breaches of it. It may investigate a complaint from an individual, though it expects the complaint to have been raised with the School first. The School is registered with the ICO as a data controller and pays the annual data protection fee.

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 is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- Data processor: an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- 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, recordings and transcripts of meetings, and minutes of meetings). The definition also 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 information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- 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 the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties). It applies to personal data in any format, including paper records, electronic files, email, images, and audio recordings and transcripts. Those who handle personal data as employees or governors 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 "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right. Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy. 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

The School has appointed the Second Master as the Data Protection Officer (DPO) who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the UK GDPR. 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 DPO. The Second Master holds this role for the whole of the School, including The New Beacon, and has day-to-day responsibility for subject access requests and for data protection complaints.

In carrying out the Data Protection Officer role the Second Master acts independently, reports to the Governors on data protection matters, and may not be penalised for advice given in that capacity. Where the role would place him in a conflict of interest, the matter is referred to the Chief Operating Officer and, if necessary, to the Chair of Governors. A conflict is likely to arise where the Second Master has decided, or would be expected to decide, the underlying matter. This includes:

- a complaint or subject access request made by or about him, or about a decision he has taken;
- a personal data breach caused by a decision or system for which he is responsible;
- a DPIA for a project he is sponsoring;
- a safeguarding or disciplinary matter in which he is the decision-maker and a data protection question arises about the same facts; and
- any case where he would in effect be reviewing his own advice.

The School has also appointed a Privacy Officer at The New Beacon, who is the first point of contact on site for pupils, parents and staff of that school. The Privacy Officer deals with routine data protection queries, records processing activities and retention for The New Beacon, and reports subject access requests, complaints and suspected personal data breaches to the DPO without delay. The Privacy Officer is not a second Data Protection Officer, because the School is a single data controller, and does not decide matters reserved to the DPO. The current holders of both roles,

and how to contact them, are published on both schools' websites and in the School's Privacy Notices.

The DPO is supported by the Director of IT & Digital, who is responsible for the technical and system aspects of data protection, for the register of approved systems and suppliers, for the register of approved AI tools, and for carrying out Data Protection Impact Assessments. Overall accountability rests with the Governors, to whom the DPO is to report annually on data protection compliance, incidents and complaints.

THE PRINCIPLES

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

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 the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies, and in particular the Record of Processing Activities which Article 30 of the UK GDPR requires the School to keep;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments);
- maintaining a retention schedule, and keeping a register of approved systems and suppliers, a register of approved AI tools, a breach log, and records of subject access requests and data protection complaints, each in the form the School is required to keep;
- generally having an 'audit trail' concerning 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 that is commonly used is consent. However, because the definition of what constitutes consent has been tightened under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground. Consent is rarely appropriate in the employment context, because of the imbalance of power between the School and its staff.

The grounds for processing personal data generally used by the School is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as 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;
- "recognised legitimate interests", which do not require a balancing assessment. The categories most relevant to the School are safeguarding children and individuals at risk, responding to emergencies, preventing crime, and disclosing personal data to another organisation, such as the police or the local authority, which needs it for its public tasks. Requests of that kind must still be referred to the DPO before anything is disclosed;
- 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.

Where the School relies on a condition in Schedule 1 of the DPA 2018 to process special category or criminal offence data, such as the employment condition or the substantial public interest conditions covering safeguarding and the prevention of unlawful acts, it must maintain an Appropriate Policy Document as required by Schedule 1, Part 4. That document must explain how the School complies with the data protection principles for that processing and how long it keeps the data. The DPO is responsible for the Appropriate Policy Document. It must be reviewed at least every two years and made available on request. The School's Appropriate Policy Document is its Special Category and Criminal Offence Data Policy.

HEADLINE RESPONSIBILITIES OF ALL STAFF

Record-keeping

Personal data held by the School must be accurate, fair and adequate. Staff must tell the School if they believe any personal data is inaccurate or untrue, or if they are dissatisfied with how it has been recorded. This applies to their own data and to the data of others, in particular colleagues, pupils and their parents, all of which must be recorded professionally. Individuals about whom staff record information on School business, whether in email, notes or hard copy files, may have the right to see it, as set out below. That must not discourage staff from making the necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies. Grounds may sometimes exist to withhold those records from a request. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies: Acceptable Use of Technology (Staff) Policy, Cyberbullying Policy, Emerging Technology and AI Policy, AI Governance Framework, Cyber Security Policy, Taking, Storing and Using Images of Pupils Policy, and Online Safety Policy. School business involving personal data must be conducted on School systems. Staff must not use personal email accounts, personal messaging applications or personal cloud storage to hold or exchange personal data about pupils, parents or colleagues; records held there remain disclosable, but cannot be properly secured, retained or retrieved by the School.

New systems, suppliers and AI tools

Staff must not adopt, purchase, subscribe to, or trial any system, application, or online service that will be used with personal data until the Director of IT & Digital approves it. This applies to free services and trials as well as paid contracts, and applies whether or not the service is accessed on a School device. Approval requires a written contract meeting the requirements of Article 28 of the UK GDPR, confirmation of where data is held and of any transfer outside the UK, and a DPIA where the processing warrants one.

AI tools follow the route set out in the School's AI Governance Framework. Anyone may propose a tool. Proposals go to IT & Digital and should not be shared with colleagues as a recommendation, because that tends to put a tool into use before it has been assessed. Only tools recorded on the register of approved AI tools may be used. Personal data must not be entered into any tool that is not on the register, and pupil, health, pastoral or safeguarding information must not be entered into any AI tool without the specific agreement of the DPO. Staff remain responsible for anything produced with the assistance of an AI tool and must check it before relying on it.

Recording and transcription of meetings

Staff must not record a meeting, or use an automated transcription or note-taking tool in a meeting, without telling everyone present first. This applies to meetings in person, on Teams and by telephone, and applies whether the tool joins the meeting itself or runs on a member of staff's device. Covert recording of colleagues, pupils, parents or third parties is not permitted in any circumstances and will be treated as a disciplinary matter. Only approved tools may be used, and not personal accounts or devices.

Some meetings must not be recorded or transcribed: confidential pastoral conversations, counselling and wellbeing sessions, medical consultations, and meetings concerning a pupil's special educational needs or Education, Health and Care Plan. A departure from this requires the agreement of the DPO in advance and must not be decided in the meeting itself.

Safeguarding and child protection meetings may be recorded only in special circumstances, only with the prior agreement of the Designated Safeguarding Lead, and only under the DSL's supervision. Before the recording is made the DSL records the decision and the reasons for it, the purpose the recording will serve, who will have access to it, where it will be stored, who it may be shared with and on what basis, and the date on which it will be reviewed for deletion. Automated transcription and AI note-taking tools must not be used in these meetings in any circumstances. Recordings are saved by the DSL in the designated location and are not held elsewhere, copied or forwarded. The Record Keeping Policy sets out how long they are kept.

Recordings and transcripts are the personal data of everyone present, are disclosable on a subject access request, and may be required in legal proceedings. Automated transcripts are often inaccurate, misattributing speakers and mishearing words, so the person chairing the meeting must check the transcript against their own notes before it is relied on. The agreed notes or minutes, and not the transcript, are the record of the meeting. Transcripts and any associated audio must then be deleted, in accordance with the retention position below.

Disciplinary, grievance, capability and investigatory meetings may be recorded only using a tool approved for that purpose, which must not retain a copy of the audio. The employee must be told in the invitation to the meeting and again at the start of it. Any objection must be recorded and the chair's decision on how to proceed documented. Further detail is set out in the School's Disciplinary and Grievance procedures.

Retention and deletion

Personal data must be kept no longer than necessary. The School's retention periods are set out in its Record Keeping Policy, which applies at both schools and covers records in any format, including audio and video recordings, transcripts and material held in cloud services. Staff must not keep personal data beyond the applicable period and must not delete records before it expires. Transcripts and any associated audio are deleted once the notes of the meeting have been agreed, and in any event within 20 working days.

Deletion must be suspended where a matter is disputed or unresolved, where a complaint, grievance, disciplinary process, investigation or legal claim is live or reasonably anticipated, or where a subject access request has been received. In those circumstances staff must preserve all relevant material, including drafts, notes, recordings and transcripts, and tell the DPO. Deleting material to prevent its disclosure once a request has been made is a criminal offence under section 173 of the DPA 2018.

Personal data breaches

A personal data breach may take many different forms, for example: the loss or theft of data or equipment on which personal information is stored; unauthorised access to or use of personal information either by a member of staff or third party; loss of data resulting from an equipment or systems (including hardware and software) failure; human error, such as accidental deletion or alteration of data, or sending an email to the wrong recipient; unforeseen circumstances, such as a fire or flood; deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours of becoming aware of them. In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If staff become aware of a personal data breach, or suspect one, they must report it to the Second Master and the Director of IT & Digital immediately, and in any event within 24 hours. This is the same route used to report a suspected cyber incident. The 72-hour deadline runs from the point at which the School becomes aware, so late internal reporting can put the School in breach even where the incident itself was minor. Staff should not attempt to investigate or resolve a suspected breach before reporting it. The School is required to record every breach, whether or not it is reported to the ICO, and the DPO is responsible for keeping that record.

If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious or minor, and it may involve fault or not, but the School always needs to know about it to make a decision. The School may not need to treat the incident itself as a disciplinary matter, but a failure to report it could expose the School and those affected, and is itself a disciplinary matter.

Care and data security

All School staff, and contractors, must keep the data protection principles in mind and comply with them whenever they 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 consider the most secure means of delivery, and the consequences of loss or unauthorised access. We expect all those with management/leadership responsibilities to uphold these principles, to see that concerns about how personal information is used are reported promptly to the DPO, and to identify and arrange the training their teams need. Staff must attend any training we require them to. Data protection training is to form part of induction and to be repeated at least every two years, with records of completion kept by HR.

Data Protection Impact Assessments

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the School is planning to use a new form of technology), we will, before commencing the processing, carry out a Data Protection Impact Assessment (DPIA) to assess: whether the processing is necessary and proportionate in relation to its purpose; the risks to individuals; and what measures can be put in place to address those risks and protect personal information. The manager responsible should contact the DPO before a new technology or a significant new processing activity is introduced.

A DPIA is required in particular where the School proposes to use a new technology, including any AI tool; process special category or criminal offence data on a significant scale; process pupils' personal data in a new system or for a new purpose; use tracking, monitoring, profiling or biometric technology; record or transcribe meetings; or use a new supplier or transfer personal data outside the UK. Enabling a new AI, recording or analytics feature within a system the School already uses counts as new processing and requires a DPIA, even where the supplier is already approved. Where a DPIA identifies a high risk that cannot be mitigated, the School must consult the ICO before the processing begins.

SAFEGUARDING AND DATA PROTECTION

Data protection law does not prevent the sharing of information for the purposes of keeping children safe. Keeping Children Safe in Education is explicit that fears about sharing information must not be allowed to stand in the way of safeguarding and promoting the welfare of children. Speak to the Designated Safeguarding Lead, who decides what is shared; what is shared must be focused and proportionate, and the decision and the reasons for it are recorded.

Children at a protected address. Where a child is in a refuge or another form of emergency accommodation, or where releasing information would be likely to cause serious harm, personal data about them is withheld rather than disclosed, including in response to a request from a parent. Any request touching a pupil in those circumstances is referred to the Designated Safeguarding Lead and the DPO before anything is sent, and it is never dealt with by the member of staff who received it.

RIGHTS OF INDIVIDUALS

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation, and may be made to any member of staff, in writing or verbally. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the Second Master as soon as possible, who leads the School's response. The School must reply within one month. Where clarification is reasonably required in order to respond, that period may be paused while it is sought, though clarification must not be requested routinely. The School is required to carry out only reasonable and proportionate searches. Once a request has been received, nothing within its scope may be deleted or amended. Individuals also have legal rights to:

- be informed about how their personal data is used, as set out in the School's Privacy Notices;
- 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;
- 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; and
- complain to the School, and to the ICO, about how their personal data has been handled.

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 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 the Second Master as soon as possible.

AUTOMATED DECISION-MAKING

The law on decisions taken solely by automated means changed in February 2026. The former general prohibition has been replaced by a framework of safeguards. Where a significant decision about an individual would be taken solely by automated processing, with no meaningful human involvement, the individual must be given information about the decision, an opportunity to make representations, the right to obtain human intervention and the right to contest the outcome. Where

such a decision would be based wholly or partly on special category data it remains prohibited unless the individual has given explicit consent or a substantial public interest condition applies.

The School does not take significant decisions about pupils, parents or staff by solely automated means. Where AI is used to support a decision, the decision itself must rest with a member of staff who has considered the case rather than approved an automated output. Staff who think a process in their area may amount to automated decision-making should raise it with the DPO.

DATA PROTECTION COMPLAINTS

Section 164A of the DPA 2018 requires the School to operate a procedure for handling data protection complaints. Any individual, whether a pupil, parent, member of staff or other person, may complain to the School if they consider that their personal data has not been handled in accordance with Data Protection Law.

Complaints may be made by email to schooladmin@tonbridge-school.org or by writing to the Second Master at Tonbridge School, Tonbridge, Kent TN9 1JP. A complaint concerning The New Beacon may be made to the Privacy Officer at that school, who will pass it to the Second Master on the same working day; complaints are handled centrally so that the School meets a single statutory timetable. A complaint need not use the word "complaint" and may be made to any member of staff. Any expression of dissatisfaction about the handling of a person's own personal data may be a complaint for these purposes.

Staff who receive anything that may be a data protection complaint must pass it to the Second Master on the same working day and must not attempt to resolve it themselves. The School must acknowledge a complaint within 30 days of receiving it, investigate without undue delay, keep the complainant informed and tell them the outcome. A record of complaints and their outcomes is to be kept by the Second Master and reported to the Governors annually. An individual who remains dissatisfied may complain to the ICO, which expects the matter to have been raised with the School first.

DATA SECURITY: ONLINE AND DIGITAL

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. If you have access to personal data, you must:

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow other staff to access personal data if they have appropriate authorisation;
- Only allow individuals who are not School staff to access personal data if you have specific authority to do so from the Second Master (DPO) or Chief Operating Officer;
- Keep personal data secure (e.g. by complying with rules on access to premises, computer access, password protection and use of Multi-Factor Authentication, secure file storage and destruction and other precautions set out in the School's Acceptable Use of Technology (Staff) Policy, Cyberbullying Policy, Emerging Technology and AI Policy, Taking Storing and Using Images of Pupils Policy, and Online Safety Policy);
- Not remove personal data, or devices containing personal data (or means which can be used to access it), from the School's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- Not store personal data on unsecured local drives or on personal devices.

Processing of Financial/Credit Card Data. The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Financial Controller. 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.

TRANSFERS OUTSIDE THE UK

Where personal data is transferred outside the UK, whether by sending it or by using a service that stores or accesses it overseas, an appropriate transfer mechanism must be in place. This will be UK adequacy regulations, the UK International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment. Staff must not put such arrangements in place themselves; they are handled by the Director of IT & Digital as part of the approval of a system or supplier.

BIOMETRIC DATA

The thermographic screening equipment described in the CCTV Policy is not in use and will not be brought back into use without a Data Protection Impact Assessment and the DPO's written agreement. The same applies to the introduction of any new system using biometrics, such as for catering, library or access control.

Biometric data used to identify a person is special category data. Where the biometric information of a pupil under 18 is to be processed, sections 26 to 28 of the Protection of Freedoms Act 2012 also apply: the School must notify each parent, must obtain the written consent of at least one parent, and must not proceed if any parent objects or if the pupil refuses, whatever the position of the parents. A pupil may withdraw at any time. An alternative means of access that does not use biometrics must always be available, and no pupil may be disadvantaged for using it. Biometric data must be used only for the purpose for which it was obtained and securely deleted when the pupil leaves the School or the system is withdrawn.

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?

Annex 1 below lists the practical points to remember, and is a useful reminder of what to do and what not to do.

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 we handle and record personal information and manage our relationships with people. This is an important part of the School's culture, and all its staff and representatives need to be mindful of it.

This policy is owned by the DPO and reviewed annually, or sooner following a significant incident or a change in the law.

ANNEX 1: Data Protection Essentials

1. Ensure you keep any personal information about other people (pupils, parents, staff, Ots, etc.) you hold secure: ensure physical files are locked away at the end of the day, don't leave personal information lying around on your desk, and don't leave your computer on, unlocked and unattended.
2. Delete (from systems) or shred personal information you no longer need, in line with the Record Keeping Policy; this may include information on prospective pupils or job applicants

(but please remember that you must not delete any pupil or staff records, and must not delete anything once a subject access request, complaint or dispute is live).

3. Don't take personal information off School premises unless necessary (e.g. when taking a School trip), and keep it secure if you do (e.g. on an encrypted memory stick); do not send or transfer personal information to your home or personal computer or device, or send personal information by email to your personal email account.
4. Keep your School login information secure, and do not use your School e-mail address and School password combination for any other services (e.g. Linked-in or Facebook).
5. Send personal data to other organisations only if necessary, and, if so, securely (i.e. in a password protected file, with the password sent separately). If you are unsure whether it is appropriate to send personal data, please check with the Second Master or Chief Operating Officer.
6. Take care when writing any document or e-mail about (or referencing) any individual: remember that they are very likely to have the right to see what you have written.
7. Do not access personal information about pupils or staff (prospective, current or past) on one of the School's systems (e.g. The Tonbridge App, iSAMS or Firefly) if you don't have a legitimate reason for doing so.
8. Report any "data breach" (i.e. the accidental destruction, loss, alteration, unauthorised disclosure of, or access to, personal information) immediately to the Second Master and to the Director of IT & Digital.
9. Contact the DPO (the Second Master) or Chief Operating Officer if you have any questions or concerns about any of the above.
10. Tell people before you record a meeting or switch on an AI notetaker, and only use a tool the School has approved. If you would not be comfortable with everyone present reading the transcript, do not record.
11. Do not put personal information into an AI tool that is not on the School's register of approved AI tools, and never put pupil, health, pastoral or safeguarding information into one.
12. If in any doubt, ask the Second Master or the Director of IT and Digital for guidance.

ANNEX 2: The New Beacon

The Data Protection for Staff Policy applies in full at The New Beacon. This annex sets out the only points at which the operational position differs, because of the age of the pupils or the arrangements on the site.

The Privacy Officer

The Second Master is the Data Protection Officer for the whole charity, including The New Beacon. The Operations Director is the Privacy Officer at The New Beacon.

A child's own rights, and parental authority

A child may exercise their own data protection rights where, in the School's reasonable opinion, they have sufficient maturity to understand the request they are making. Most pupils at The New Beacon are below that point, so a request is normally made by a person with parental responsibility on the child's behalf. Where a pupil in Year 7 and 8 makes a request in their own right, or where the information concerns something the pupil has raised in confidence, the DPO decides who receives what, having regard to the child, the information requested and the circumstances.

Where the School relies on consent for an online service used by pupils, the consent of a person with parental responsibility is required for a child under 13, under Article 8 of the UK GDPR as applied by section 9 of the DPA 2018.

The Early Years

The Nursery and Reception are subject to the statutory framework for the Early Years Foundation Stage, which requires the School to keep records of attendance, accidents, the administration of medicines and the assessment of a child's development, and to have a policy on the use of mobile telephones and cameras in the setting.
Information about a child in the Early Years is shared with a person with parental responsibility as a matter of course. Where sharing would put the child at risk, the decision is for the Designated Safeguarding Lead.

Photographs and images of younger pupils

The School relies on legitimate interests for photographs of pupils at both schools, as set out in the Taking, Storing and Using Images of Pupils Policy and the Privacy Notices, and a parent or pupil may object at any time. Article 6(1)(f) of the UK GDPR requires the interests and fundamental rights of the individual to be weighed, and gives particular weight to those of a child. At The New Beacon the School therefore applies the following restrictions:

- a pupil's full name is not published with their image;
- images of pupils in the Nursery and Reception are used within the School and in communication with parents, and are not used in external advertising, in the press or on public social media channels without the specific permission of a person with parental responsibility;
- images are not used in a way that identifies where a particular child can be found at a particular time; and
    - a written record is kept of any parent who has objected, and that objection is honoured permanently, including after the pupil moves up to Tonbridge.

Objections recorded at The New Beacon before September 2026 continue to be honoured, whether they were given as a refusal of consent or otherwise.

CCTV at The New Beacon

The New Beacon has a closed-circuit television system, installed in 2026 and managed by Tonbridge School, to which the CCTV Policy applies in full. The Operations Manager at The New Beacon holds access on site and is to be recorded on the list of authorised viewers for the site alongside the Tonbridge post holders named in that policy.
The record of camera locations, the identity of the System Manager and the list of authorised viewers are kept separately for The New Beacon. Signage on the site is to identify Tonbridge School as the data controller. No cameras are placed in the Nursery and Early Years areas, in sleeping accommodation, or in medical, counselling, changing or washroom facilities.

Records when a pupil leaves

A pupil moving from The New Beacon to Tonbridge remains within the same legal entity and the same data controller. Transferring their records is internal processing rather than disclosure to a third party, so no data-sharing agreement is required, and the requirement in Keeping Children Safe in Education to pass a child protection file to a new school does not apply. Retention periods continue to run from the same starting point.

Where a pupil moves to another school or college, the child protection file is provided to that school as Keeping Children Safe in Education requires; the School retains its copy in accordance with the Record Keeping Policy, and any other transfer of records is a disclosure to a separate controller.