DATA PROTECTION POLICY

1. Background

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

UK Data Protection Law consists primarily of the UK version of the General Data Protection Regulation (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. The UK GDPR substantially repeats the EU GDPR to which we were subject before 1 January 2021 and which may still apply to some of our data processing and responsibilities.

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 the UK's independent regulatory authority and is responsible for enforcing data protection law. The ICO has the power to look into individuals' complaints without cost, and has various powers to take action for breaches of the law.

2. Definitions

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

- **Data Controller** – the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR. The School (including by its governors) is a Data Controller. An independent contractor who makes their own such decisions is also, separately, likely to be a Data Controller.

- **Data Processor** – a person or 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.

- **Data Subject** – a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

- **Personal Data Breach** – any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

- **Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Person Data includes Special

Categories of Personal Data and pseudonymised Personal Data but excludes anonymous data or data that has had the identify of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual.

- **Processing** –any activity that involves the use of Personal Data. It includes obtaining or collecting it, structuring it, analysing it, amending it, recording, holding or storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it, retrieving, using, disclosing, deleting or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

- **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.

3. 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).

Employees and governors of the School who handle personal data 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 risks to the School or individuals will be considered a serious matter and may lead to disciplinary action.

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

Where the School shares personal data with third party Data Controllers or Data Processors – which may include other schools, parents, appropriate authorities, 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.

4. Person responsible for Data Protection at the School

The School has appointed Stephen Robinson (Business Director) as the "**Data Protection Lead"** 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 Data Protection Lead.

Where this policy asks you to refer or report to Stephen Robinson you should use the email address dataprocessing@tringpark.com wherever practicable.

5. The Principles

Principles relating to the processing of personal data set out in the UK GDPR 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, explicit and legitimate purposes and only for the purposes it was collected for;
3. Adequate, relevant and limited to what is necessary for the purposes for which it is processed;
4. Accurate and where necessary kept up to date;
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which it is processed;
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage of the Personal Data;
7. Not transferred to another country without appropriate safeguards in place; and
8. Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their 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;
- documenting significant decisions and assessments about how we use Personal Data (including via formal risk assessment documents called Data Protection Impact Assessments); 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).

6. 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, because the definition of what constitutes consent has been tightened under 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 where possible.

One of these alternative grounds is 'legitimate interests'. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School.

Other lawful grounds upon which the School may rely, in addition to consent and legitimate interest 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;
- to protect the Data Subject's vital interests;

There are other rules relating to the processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. Headline responsibilities of all staff

Record-keeping

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

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

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 the staff handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies in particular:

- CCTV
- Data Security Breach
- Online safety IT and Acceptable Use
- Privacy Notice Parents & Pupils
- Safeguarding Policy
- Staff Code of Conduct
- Taking, Storing and using Images of Pupils
- Remote working

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 a Personal Data Breach

One of the key obligations contained in the UK GDPR is on reporting Personal Data Breaches. Data Controllers must report certain types of Personal Data Breach (those which risk an impact to individuals) to the ICO within 72 hours.

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 they must notify the Data Protection Lead, Stephen Robinson Business Director. If staff are in any doubt as to whether to report something internally, it is always best to do so. A Personal Data Breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs the information to make a decision.

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

Care, data security and training

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use their best efforts to comply with those principles whenever they process Personal Data. Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. All staff handling data 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 personal information is used by the School to the Data Protection Lead, Stephen Robinson, Business Director.

The School are required to ensure that all Staff have undergone adequate training to enable them to comply with data privacy laws. The School must also regularly test our systems and processes to assess compliance. Those with management/ leadership responsibilities must also identify the need for (and implement) regular staff training. Staff must attend any training we require them to attend.

Staff must regularly review all the systems and processes under their control to ensure that they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

8. Rights of Individuals

In addition to the School's responsibilities when Processing Personal Data, individuals have certain specific rights, perhaps most significantly the right to request access to their Personal Data held by a Data Controller (i.e. the School). This is sometimes 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 the Data Protection Lead, Stephen Robinson, Business Director immediately as there are timeframes within which to respond that start as soon as the request is received.

Data Subjects have rights when it comes to how the School handles their Personal Data. This includes rights to:

- Withdraw consent to Processing at any time;
- Receive certain information about the School's Processing activities;
- Prevent our use of their Personal Data for direct marketing purposes;
- 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 if it is no longer necessary in relation to the purposes for which it was collected or processed);
- request that we restrict our data Processing activities (in certain circumstances);
- in limited circumstances, receive from us or ask for the Personal Data we hold about them to be transferred to a third party in a structured, commonly used and machine-readable format;
- object, on grounds relating to their particular situation, to any of our particular Processing activities where it is likely to cause damage or distress to the Data Subject or anyone else;
- object to Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the UK;
- object to decisions based solely on Automated Processing, , including profiling (i.e. where a significant decision is made about the individual without human intervention);
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority.

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 Data Protection Lead, Stephen Robinson, Business Director as soon as possible.

9. 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.

- no member of staff is permitted to remove Personal Data from the school premises, whether in paper or electronic form and wherever stored, without prior consent of the Principal

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

- It is not permitted to take data off-site

- Use of personal email accounts or unencrypted personal devices by governors or staff for official School business is not permitted.

10. Processing of Financial/Credit Card Data

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

11. Policy Statement

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 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 to 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.