Cayman Prep & High School

WHOLE SCHOOL

Data Protection Policy

School Mission Statement:

At Cayman Prep and High School, we aim to provide a stimulating learning environment, firmly rooted in Christian principles, in which our students become critical creative thinkers, responsible citizens and lifelong learners in an ever-changing world".

Core Values:

Loyalty	***Forgiveness***
Self-Discipline	***Empathy***
Integrity	***Friendship***
Excellence	***Caring***
Respect	***Communication***

Contents:

1 Background
2 Data Protection Lead
3 The Principles
4 Lawful grounds for data processing
5 Headline responsibilities of all staff
6 Rights of individuals
7 Data Security: online and digital
8 Processing of Credit Card Data
9 Summary

DATA PROTECTION POLICY

1. Background

Data protection is a legal requirement for Cayman Prep and High School (the "**School**"). During the course of the School's activities, it collects, stores and processes Personal Data (sometimes sensitive in nature) about staff, students, their parents, suppliers and other third parties (fully detailed in the School's Privacy Notice, a copy can be found on the School Website, under useful information. All staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether the data is personal and of a sensitive nature or routine.

The Data Protection Act 2017 came into force on 1st September 2019 and is analogous to the UK Data Protection Act 2018 and the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") effective as of 25 May 2018. The Data Protection Act (2021 Revision) is the current law in the Cayman Islands and aims to protect individual's rights in relation to their personal data and is based upon, and seeks to provide equivalent protection, to the GDPR. In the context of our safeguarding obligations, the School has a heightened duty to ensure that the personal data of students is at all times managed responsibly and securely.

The act sets out the legal grounds in this area and strengthens the rights of individuals by placing tougher compliance obligations on organisations including schools that manage personal information. The Cayman Islands Ombudsman is responsible for enforcing the data protection ~~law~~ act and has powers to act for breaches of the law.

Those who engage in the processing of personal data are obliged to comply with this policy. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action.

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (e.g., including parents, students, employees).

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

- **Breach** – means a Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data transmitted, stored or otherwise proceeded, whether manual or automated
- **Data** – includes both automated and manual Data. Automated Data means Data held on computer, or stored with the intention that it is proceed on a computer.
- **Data Controller** – an organisation that determines the purpose and means of the Processing of Personal Data. For example, the School is the controller of students' personal information. As a Data Controller, the School is responsible for safeguarding the use of personal data.

- **Personal Data**: means any information relating to a living individual (a data subject) who can be identified, directly or indirectly from such Data. For example, names, identification number, email addresses, IP addresses and mobile phone numbers. Descriptions of individuals with sufficient specificity will also be considered Personal Data such as in emails, notes of calls and minutes of meetings Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- **Processing** –means any use of Personal Data. For example: storage in databases, input onto systems and applications, sharing with law enforcement and creating accounts.
- **Processor** – an organisation that Processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.
- **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.

2. Data Protection Lead

The Business Manager is the Data Protection Lead and will endeavour to ensure that all Personal Data is processed in compliance with this Policy and the principles of the 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.

3. The Principles

The Act sets out eight 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 for which it was collected.

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.

6. **Used in accordance with the rights of the individuals**, as specified in the law.

7. Processed in a manner that ensures **appropriate security** of the Personal Data.

8. **Must not be transferred abroad** unless an adequate level of protection can be guaranteed.

The ‘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; 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, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

4. Lawful grounds for data processing

Under the act, 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, it is considered preferable to 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 Controller. Data subjects can challenge it and means the Controller 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.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and equality.
- contractual necessity, e.g., to perform a contract with staff or parents.
- 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.

5. Headline responsibilities of all staff

<u>Record-keeping</u>

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School if you believe that *your* Personal Data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record

the Personal Data of others – in particular, colleagues, students and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business 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 students, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to record every document or email in such a way that you would be able to stand by it if the person about whom it was recorded were to see it.

Data handling

All staff have a responsibility to manage 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. 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, sign and comply with the following policies:

- Network Acceptable Use Agreement.
- E-Safey and Acceptable Use Policy.

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 new obligations 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 Cayman Islands Ombudsman within five days.

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 Office. If you become aware of a Personal Data breach, you must notify the school's business manager and the School Data Protection Lead (see Section 2 above). If staff are in any doubt as to whether you should report something, it is always best to do so. A Personal Data breach may be serious, or it may be minor, and it may involve fault or not, but the School always needs to know about them to decide.

The School may not 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 staff member's contract.

Care and Data security

More generally, we require all School staff to remain conscious of the data protection principles (see section 3 above), to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Staff 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 adhere to these principles and to oversee the timely reporting of any concerns about how personal information is used by the School to the School Data Protection Lead (see Section 2 above). and to identity the need for (and implement) regular staff training.

6. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, most significantly that of access to their personal data held by a data controller (i.e., the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the School Data Protection Lead (see Section 2 above) as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate.
- request that we erase their Personal Data (in certain circumstances).
- request that we restrict our data processing activities (in certain circumstances).
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another Data Controller.
- object, on grounds relating to their situation, to any of our Processing activities where the individual feels this has a disproportionate impact on them; and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we are relying on it for Processing their Personal Data.

Except for the final bullet point, none of these rights for individuals are unqualified and exceptions may well apply. 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 School Data Protection Lead (see Section 2 above) as soon as possible.

7. 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. As such, no member of staff is permitted to remove Personal Data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the appropriate school principal. [Where a worker is permitted to take data offsite it will need to be encrypted.] Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

8. Processing of Credit Card Data

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

9. Summary

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

Ask yourself the following questions:

- *Would I be happy if my own Personal Data 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?*

The Data Protection Act (as revised) is a code of useful and sensible checks and balances to improve how to manage and record Personal Data and to 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."