DATA PROTECTION POLICY

1. Background

Data protection is an important legal compliance issue for The Ladies' College, Guernsey comprising Melrose (including the Pre-School), the Senior School and the Sixth Form (together the "**College**"). During the course of the College's activities it collects, stores and processes personal data (sometimes sensitive in nature) about current, past and prospective students, their parents and siblings, employees, contractors, volunteers and other third parties (in a manner more fully detailed in the College's Privacy Notice which is available on the College website). For the purposes of this policy, references to "**students**" means pupils of Melrose and students of the Senior School and the Sixth Form, "**parents**" shall include guardians and carers and "**colleagues**" shall include employees and contractors of the College (as the case may be).

The College, as "**data controller**", is liable for the actions of its colleagues and governors in how they handle data. It is therefore an area where all colleagues have a part to play in ensuring they and the College comply with, and are mindful of, our legal obligations, whether that personal data handling is sensitive or routine.

The Data Protection (Bailiwick of Guernsey) Law, 2017 (the "**DP Law**") is directly effective in Guernsey. The DP Law 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.

Without fundamentally changing the principles of data protection law and while providing some helpful new grounds for processing certain types of personal data, in most ways, data protection legislation has strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Office for Data Protection Authority (the "**ODPA**") is responsible for enforcing data protection law in Guernsey. It will typically look into individuals' complaints, routinely and without cost, and it has various powers to take action for a breach of the law.

If any provisions of this policy are or may appear to be inconsistent with the provisions of any other relevant policy or procedure, the provisions of this policy shall apply, as appropriate.

2. 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 its governors) is a data controller. An independent contractor who makes their own decisions on such matters is likely to be, also, separately, 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 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, collecting, structuring, analysing, storing, altering or deleting it or sharing it, internally or with third parties (including making it available to be viewed electronically or otherwise).

- "**special category data**" **–** personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, personal data concerning an individual's sex life or sexual orientation or health, genetic or biometric data used to identify an individual. (Biometric and genetics special category data is not currently relevant for the purposes of the College.) 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 College's expectations and procedures with respect to processing any personal data we collect from data subjects (including current, past and prospective students, their parents and siblings, colleagues, contractors, volunteers and third parties).

Those who handle personal data as colleagues or governors of the College are obliged to comply with this policy when doing so. For colleagues, 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 "data processors" on the College'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 College shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to contractors 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 a 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 College

The College has appointed the Bursar as the Data Protection Officer, who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the DP Law. 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 Officer. The College has also appointed the Head of Curriculum IT and E-Safety and the Network Manager each of whom has key practical responsibility for the storage of personal data.

5. The Principles

The DP Law 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, 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 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 DP Law's seventh, broader '**accountability**' principle also requires that the College 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 ("**DPIA**")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including, for example, when and how our Privacy Notice is updated; when colleagues' 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.

6. Lawful grounds for data processing

Under the DP Law 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 DP Law (and the fact that it can be withdrawn by the data subject), it is considered preferable for the College 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 College. It can be challenged by data subjects and also means the College is taking on extra responsibility for considering and protecting people's rights and interests. The College's legitimate interests are set out in its Privacy Notice, as the DP Law 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 employees or parents, or the engagement of contractors;
- a narrower set of grounds for processing special category data (such as health information), which includes explicit consent, emergencies and specific public interest grounds.

7. Headline responsibilities of all colleagues

Record-keeping

It is important that personal data held by the College is accurate, fair and adequate. Colleagues are required to inform the College if they believe that *any* personal data is inaccurate or untrue or if they are dissatisfied with how it is recorded. This applies to how colleagues record their own data, and the personal data of others – in particular, other colleagues, students and their parents – in a way that is professional and appropriate.

Colleagues 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 colleagues from recording necessary and sometimes difficult records of incidents or conversations involving other colleagues or students, in accordance with the College's other policies; and grounds may sometimes exist to withhold these from such requests. However, the starting position for colleagues 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 colleagues 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 College policies and procedures (to the extent applicable to them). 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 all colleagues should read and comply with relevant policies including the following:

- the Child Protection (Safeguarding) Policy;
- the ICT Policy, which includes an Acceptable Use Policy (AUP) for students, codes of conduct for colleagues and students and an E-Safety Policy, including the use of images;
- the CCTV Policy;
- the Taking, Storing and Using Images of Children Policy.

Responsible processing also extends to the creation and generation of new personal data or 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 DP Law 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 ODPA within 72 hours after becoming aware of the breach.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to (amongst other things) their rights and freedoms. In any event, the College must keep a record of any personal data breaches, regardless of whether we need to notify the ODPA. If colleagues become aware of a personal data breach they must notify the Data Protection Officer. If colleagues 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 College always needs to know about them in order to decide about next steps.

As stated above, the College 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 colleague's contract.

Care and data security

More generally, we require all College colleagues (and expect all our contractors) to remain mindful of the data protection principles (see section 5 above), 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 affects daily processes: such as 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. To that end, colleagues must:

- at all times take care to ensure the safe-keeping of personal data, minimising the risk of loss or misuse;
- not remove personal data from the College premises or its official ICT systems, whether in paper or electronic form and wherever stored, without prior consent of the Principal;

- use personal data only on secure password protected devices, ensuring screens are locked or that they are properly logged-off a device when they leave a room or at the end of any session;
- not transfer sensitive / special category data unless that data is encrypted, redacted or the personal identifier is held separately to the data, so it cannot be attributed and secure password protected devices are used.

The College will take reasonable steps to ensure that colleagues will only have access to personal data relating to students or their parents/carers where it is necessary for them to do so.

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 College to the Data Protection Officer, and to identity the need for (and implement) regular training for colleagues. Colleagues must attend any training we require them to.

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 Guernsey data protection law). 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 the Data Protection Officer in the first instance, and at as early a stage as possible.

8. Rights of individuals

In addition to the College'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 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 a colleague becomes aware of a subject access request (or indeed any communication from an individual about their personal data), they must tell the Data Protection Officer 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 particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if any colleague receives a request from an individual who is purporting to exercise one or more of their data protection rights, they must tell the Data Protection Officer as soon as possible.

9. 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. In complying with applicable policies, the following are of particular note:

- colleagues must take appropriate precautions to safeguard data stored on the official College ICT systems from unauthorised access and must not work in public or access sensitive or special category data in non-secure locations or on non-secure networks;
- colleagues should undertake any digital communications with a student or parent via the College's official ICT systems and (when communicating with a student) by using the student's College email address (and not their private email address) or other College message system;
- colleagues and volunteers must not disclose any personal data that they may have access to or be in possession of, as part of their professional duties, to any third parties without express permission from the Principal.

10. Processing of Financial Data

Categories of financial information, including bank details and salary, or information commonly used in identity theft (such as social insurance numbers or passport details), may not be treated as legally sensitive but can have a material impact on individuals and should be handled accordingly.

11. Notify College of changes to personal details

Parents and students (as the case may be) are asked to please notify the College of any changes to any of their personal details at the appropriate time, so that our records can be amended accordingly. We may also ask for verification of the personal details annually and

will amend any inaccuracies or changes, when the detail is returned. We shall be entitled to rely on the most recent form or declaration containing relevant information (and any subsequent updates to it) that the College holds, even if a formal confirmation or declaration is requested by the College and not returned.

12. Why we have this policy

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 a person comes 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 as a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people; it should not be seen as oppressive red tape, or a reason not to do something necessary or important.

This is an important part of the College's culture and all our colleagues and representatives need to be mindful of it.

Date: 15 June 2020

Last update: 29 November 2024