PRETORIA
BOYS HIGH SCHOOL

Data Protection Policy

1. Purpose and scope

1.1 This policy provides a framework for ensuring that the school meets its obligations under the Promotion of Access to Information Act, Act 2 of 2000 ("PAIA"), the Protection of Personal Information Act, Act 4 of 2013 ("POPI") and associated legislation.

1.2 It applies to all processing of personal data carried out for a School purpose, irrespective of whether the data is processed on non-school equipment or by third parties.

1.3 More stringent conditions apply to the processing of special category personal data.

1.4 This policy should be read in conjunction with the accompanying guidance, which provides further detail and advice on practical application, as well as any other documents that impose confidentiality or data management obligations in respect of information held by the School.

1.5 This policy does not cover the use of personal data by members of the School when acting in a private or non-School capacity.

2. Background

2.1 The processing of personal data underpins almost everything the School does. Without it, students cannot be admitted and taught; staff cannot be recruited; living individuals cannot be researched; and events cannot be organised for alumni or visitors.

2.2 We are responsible for handling people's most personal information. By not handling personal data properly, we could put individuals at risk.

2.3 There are also legal, financial and reputational risks for the School. For example:

- If we are not able to demonstrate that we have robust systems and processes in place to ensure we use personal data properly we might lose our ability to carry out research projects requiring access to personal data.
- Reputational damage from a breach may affect public confidence in our ability to handle personal information.
- The South African Courts, which enforce data privacy legislation, have the power to fine organisations for serious breaches.

3. Principles

3.1 The processing of personal data must comply with data privacy legislation and they require that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up-to-date;
- not kept for longer than necessary; and
- kept safe and secure.

3.2 In addition, a new accountability principle requires us to be able to evidence compliance with these principles.

4. Aims and commitments

4.1 The School handles a large amount of personal data and takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, it is committed to:

- complying fully with data privacy legislation;
- where practicable, adhering to good practice, as issued by the IO or other appropriate bodies; and
- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

4.2 The School seeks to achieve these aims by:

- ensuring that staff, students and other individuals who process data for School purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to data privacy legislation and the School's data protection policy;

- providing suitable training, guidance and advice. The School's online training course on data privacy and information security is available to all members of the School. The online course is supplemented by bespoke on-site training, where appropriate, along with regular talks and presentations at School conferences and departmental meetings.

- incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the concept of 'privacy by design');

- operating a centrally coordinated procedure (in order to ensure consistency) for the processing of subject access and other rights based requests made by individuals; and

- investigating promptly any suspected breach of data privacy legislation; reporting it, where necessary, to the IO; and seeking to learn any lessons from the incident in order to reduce the risk of recurrence.

5. Roles and responsibilities

Council

The School Governing Body and School Management has executive responsibility for ensuring that the School complies with data privacy legislation. It is supported by all executive personnel, which are responsible for keeping under review the School's policies and compliance with legislation and regulatory requirements.

Information Officer (IO)

The IO is responsible for monitoring internal compliance, advising on the School's data protection obligations and acting as a point of contact for individuals and the IO.

Information Compliance Team

The Information Compliance Team is responsible for:

- establishing and maintaining policies and procedures at a central level to facilitate the School's compliance with data privacy legislation;
- establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;
- supporting privacy by design and privacy impact assessments;
- responding to requests for advice from departments;
- coordinating a School-wide register exercise to capture the full range of processing that is carried out;
- complying with subject access and other rights based requests made by individuals for copies of their personal data;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and
- keeping records of personal data breaches, notifying the IO of any significant breaches and responding to any requests that it may make for further information.

In fulfilling these responsibilities, the team may also involve, and draw on support from, representatives from sections, departments and divisions.

Heads of department (or equivalent)

Heads of Department are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with the Department who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of staff to the requirements of this policy, ensuring that staff who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities.

- adequate records of processing activities are kept (for example, by undertaking register exercises);

- data protection requirements are embedded into systems and processes by adopting a 'privacy by design' approach and undertaking privacy impact assessments where appropriate;

- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;

- data sharing is conducted in accordance with School guidance;

- requests from the Information Compliance Team for information are complied with promptly;

- data privacy risks are included in the department's risk management framework and considered by senior management on a regular basis; and

- departmental policies and procedures are adopted where appropriate.

Others processing personal data for a School purpose eg. staff, students and volunteers

Anyone who processes personal data for a School purpose is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance, procedures, and/or training introduced by the School to comply with data privacy legislation. For detailed guidance, they should refer to the School's Guidance on Data Protection and any relevant departmental policies and procedures. In summary, they must ensure that they:

- only use personal data in ways people would expect and for the purposes for which it was collected;

- use a minimum amount of personal data and only hold it for as long as is strictly necessary;

- keep personal data up-to-date;

- keep personal data secure, in accordance with the School's Information Security Policy;

- do not disclose personal data to unauthorised persons, whether inside or outside the School;

- complete relevant training as required;

- report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;

- seek advice from the Information Compliance Team where they are unsure how to comply with data privacy legislation; and

- promptly respond to any requests from the Information Compliance Team in connection with subject access and other rights based requests and complaints (and forward any such requests that are received directly to the Information Compliance Team promptly).

6. Breaches of data privacy legislation

6.1 The School will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the IO. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal data is used in a way that the individual does not expect.

6.2 Incidents involving failures of IT systems or processes must be reported to the PBHS IT Department within four working hours of discovery. IT will liaise, as appropriate, with the Information Compliance Team.

6.3 All other incidents must be reported directly to the Information Compliance Team at the earliest possible opportunity.

7. Compliance

7.1 The School regards any breach of data privacy legislation; this policy; or any other policy and/or training introduced by the School from time to time to comply with data privacy legislation, as a serious matter, which may result in disciplinary action.

7.2 Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of the School to disclose personal information unlawfully).

8. Further information

Questions about this policy and data privacy matters in general should be directed to the Information Compliance Team at info@boyshigh.com.

9. Review and development

9.1 This policy, and supporting guidance, will apply with effect from 1 June 2022. It will be reviewed during the 2023 academic year to take into account outstanding IO guidance and the final form of national legislation underpinning POPI.