BRIGHTON COLLEGE
BANGKOK · VIBHAVADI

Data Protection Policy (PDPA)

This policy applies to:
Brighton College Bangkok Vibhavadi

This is an employee policy and applies to:
All staff / employees

Policy owner:	Neil Hayward
Frequency of review:	At least annually
Dates of previous reviews:	August 2025
Date of current live version:	**August 2025**
Date of next formal review:	June 2026
BCBV Policy reference:	tbc
Linked policies/documents:	The policy list as noted in point 28 of this Policy.
Key changes to previous version:	

	Name (role):	Signature:	Date:
Policy owner:	Neil Hayward	Neil Hayward	14.8.25
Ratification (Governor):			

Introduction

1. This policy is addressed to all staff and explains the College's expectations of staff under data protection legislation. It provides an explanation of key data protection.
2. Data protection is about regulating the way that the College uses and stores information about identifiable people (**Personal Data**). It also gives people various rights regarding their data - such as the right to access the Personal Data that the College holds on them.
3. As a College, we collect, store and process Personal Data about our staff, pupils, parents, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in the College.
4. You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.
5. All queries concerning data protection matters should be raised with the PDPA Lead.
6. The Thailand Personal Data Protection Act 2019 (PDPA) was published on May 27, 2019 in the Royal Thai Government Gazette. The PDPA is the first law governing data protection in Thailand, and came into full effect on 1 June 2021.
7. Brighton College Bangkok Vibhavadi International School is registered with the Ministry of Education under registration reference: 1110700039.
8. The Thailand Personal Data Protection Act 2019 (PDPA) applies to the keeping and processing of Personal Data, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, pupils and their parents/guardians how their data will be treated.

Application

9. This policy is aimed at all staff working in the College (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities. It includes employees, governing body, contractors, agency staff, work experience pupils and volunteers.
10. This policy does not form part of your contract of employment and may be amended by the College at any time.

What information falls within the scope of this policy

11. Data protection concerns information about individuals.
    11.1 Data means information in a form that can be processed. It includes both automated data (e.g. electronic data) and manual data. Automated data means any information on computer, or information recorded with the intention that it be processed by computer. Manual data means information that is kept/recorded as part of a relevant filing system or with the intention that it forms part of a relevant filing system.
12. Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available. Information as simple as someone's name and address is their Personal Data.
    12.1 Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller i.e. the school.

13. In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data. Examples of places where Personal Data might be found are:

13.1 on a computer database;
13.2 in a file, such as a pupil report;
13.3 a register or contract of employment;
13.4 pupils' exercise books, coursework and mark books;
13.5 health records; and
13.6 email correspondence.

14. Examples of documents where Personal Data might be found are:
14.1 a report about a child protection incident;
14.2 a record about disciplinary action taken against a member of staff;
14.3 photographs of pupils;
14.4 a recording of a job interview;
14.5 contact details and other personal information held about pupils, parents and staff and their families;
14.6 contact details of a member of the public who is enquiring about placing their child at the College;
14.7 financial records of a parent;
14.8 information on a pupil's performance; and
14.9 an opinion about a parent or colleague in an email.

15. Staff records:

Categories of staff data: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details,
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to Child Protection Procedures).

16. You must be particularly careful when dealing with Personal Data which falls into any of the categories below:
16.1 information concerning child protection matters;
16.2 information about serious or confidential medical conditions and information about special educational needs;
16.3 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
16.4 financial information (for example about parents and staff);
16.5 information about an individual's racial or ethnic origin;
16.6 political opinions;
16.7 religious beliefs or other beliefs of a similar nature;
16.8 trade union membership;
16.9 physical or mental health or condition;
16.10 sexual life;
16.11 sexual orientation;
16.12 genetic information;

16.13 information relating to actual or alleged criminal activity; and

16.14 biometric information (e.g. a pupil's fingerprints following a criminal investigation).

17. These categories are referred to as **special categories of personal data** in this policy and in the Information Security Policy. If you have any questions about your processing of these categories of Personal Data please speak to the PDPA lead.

Your obligations

Personal Data must be processed fairly, lawfully and transparently

18. "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

19. People must be told what data is collected about them, what it is used for and who it might be shared with, unless it is obvious.

20. If you are using Personal Data in a way which you think an individual might think is unfair please speak to the PDPA Lead.

21. You must only process Personal Data for the following purposes:

21.1 ensuring that the College provides a safe and secure environment;

21.2 providing pastoral care;

21.3 providing education and learning for our pupils;

21.4 providing additional activities for pupils and parents (for example activity clubs);

21.5 protecting and promoting the College's interests and objectives (for example fundraising);

21.6 safeguarding and promoting the welfare of our pupils;

21.7 to fulfil the College's contractual and other legal obligations; or

21.8 as outlined in the relevant privacy notices(s).

22. If you want to do something with Personal Data that is not on the above list or is not set out in the relevant privacy notice(s), you must speak to the PDPA Lead before you do anything. This is to make sure that the College has identified a lawful reason for using the Personal Data.

23. We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the PDPA Lead if you think that you may need to obtain consent.

You must only process Personal Data for limited purposes and in an appropriate way.

24. For example, if pupils are told that they will be photographed to enable an external examiner to recognise them, you should not use those photographs for another purpose (e.g. in the College's prospectus); you should also not access a colleague’s personal details from iSAMS to use for purposes not connected with the College.

Personal Data held must be adequate and relevant for the purpose

25. This means not making decisions based on incomplete data. For example, when writing reports, you must make sure that you are using all of the relevant information about the pupil.

You must not hold excessive or unnecessary Personal Data

26. Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a pupil's siblings if that Personal Data has some relevance, such as where the sibling is also a pupil, allowing the College to determine if a sibling fee discount is applicable or because the sibling (where old enough to make their own decisions) or the parent has indicated the sibling may join the school in the future.

The Personal Data that you hold must be accurate

27. You must ensure that Personal Data is complete and kept up to date. For example, if a parent notifies you that their contact details have changed, you must ask them to inform the school office so that this information is updated on iSAMS.

You must not keep Personal Data longer than necessary

28. The College has a Retention and Deletion Schedule which gives details of how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

You must keep Personal Data secure

29. Locations of data:

In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Computer records are kept on password protected PCs and cloud based storage is protected by state of the art security and enhanced data protection and controlled password protected access to information, relevant to each staff member's role/duties.

Personal devices must not contain any images of pupils or parents. Any photographs taken must be transferred to a school drive within 48 hours, and then deleted from personal devices (Child Protection Policy).

30. You must comply with the following College policies and guidance relating to the handling of Personal Data:

You must not transfer Personal Data outside of Thailand without adequate protection

31. If you need to transfer Personal Data to one of the Brighton College International schools or partners (for example, providing staff information or photos containing pupil images) please speak to the Commercial Director of BCI.

Sharing Personal Data outside the College - dos and don'ts

32. Please review the following dos and don'ts:

32.1 DO share Personal Data on a need to know basis and think about why it is necessary to share data outside of the College. In particular, in relation to safeguarding, Government guidance is explicit that data protection rules *"**do not** prevent the sharing of information for the purposes of keeping children safe and promoting their welfare … Fears about sharing information **must not** be allowed to stand in the way of the need to safeguard and promote the welfare of children."*

DO NOT send emails which contain special categories of personal data described above without taking steps to ensure that the data cannot be accessed by anyone other than the intended recipient.

32.2 DO be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations.

32.3 DO be aware of “phishing”. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords.

32.4 DO NOT reply to email, text, or pop-up messages that ask for personal or financial information, or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

32.5 DO NOT disclose Personal Data to the Police without permission.

32.6 DO NOT disclose Personal Data to contractors without permission.

Disposal of records

33. Personal data must be disposed of in a way that protects the ‘rights and freedoms’ of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Sharing Personal Data within the College

34. This section applies when Personal Data is shared within the College.
35. Personal Data must only be shared within the College on a "need to know" basis.
36. Examples of sharing which are likely to be compliant with data protection legislation include:
    36.1 a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);
    36.2 informing an exam invigilator that a particular pupil suffers from panic attacks; or
    36.3 disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).
37. Examples of sharing which are unlikely to be compliant with data protection legislation include:
    37.1 The Heads of School being given access to all pupil records kept by the Medical Centre (seniority does not necessarily mean a right of access);
    37.2 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff (unless the member of staff has given permission or it is an emergency).

You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please contact the Designated Safeguarding Lead.

Individuals' rights in their Personal Data

38. People have various rights in their information.
39. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the PDPA Lead. Please let them know by contacting them by phone or email (either for themselves or on behalf of another person, such as their child):
    39.1 wants to know what information the College holds about them or their child;
    39.2 asks to withdraw any consent that they have given to use their information or information about their child;
    39.3 wants the College to delete any information;
    39.4 asks the College to correct or change information (unless this is a routine updating of information such as contact details);

39.5 asks for electronic information which they provided to the College to be transferred back to them or to another organisation;

39.6 wants the College to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the College newsletter or alumni events information; or

39.7 objects to how the College is using their information or wants the College to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

Breach of this policy

40. Any breach of this policy will be taken seriously and may result in disciplinary action.

41. A member of staff who deliberately or recklessly discloses Personal Data held by the College without proper authority is guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

Appendix A : Implementation arrangements, roles and responsibilities

The following personnel have responsibility for implementing the Data Protection Policy:

Name	**Responsibility**
Board of management/School:	Data Controller
Admin/Academic	Data Processors Aey/CWI
Headmaster	Implementation of Policy - CWA
Head of Senior:	Data Protection Officer - NHA
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Appendix B: Short Checklist

Admin Complicance

A clear desk approach.

No paperwork that contains personal data should be visible on the desk, shelves or elsewhere in the classroom.

All paperwork containing personal data should be in a file or in a cupboard/filing cabinet.

If paperwork containing personal data is taken on trips, it must be kept secure by the trip leader, and either filed or destroyed on return to the school.

Disposal of paperwork containing personal data

Shredded, by hand or using a shredder (in HR office).

Computers

Desktop computers should not be left on when you are not in the room.

Switch user, sign out when you leave the room (Ctrl, alt, delete, enter to lock or Windows Key + L)

Set the computer to sleep mode after 3 minutes of inactivity in case you forget.

Personal emails

Do not access personal emails on school computers or devices.

Sharing documents

Avoid sharing documents with everyone in an organisation, unless it is essential
Use BCC in emails to more than one Parent, to avoid them being able to see each other's addresses.
Avoid reply all to emails or shared documents, unless it is essential
Photographs of pupils on personal devices deleted after 48 hours, after being moved to a school account.

What to do….

- If you see any personal data left out, put it in a drawer and inform the relevant person where it is.
- If you see a computer still logged in by a colleague, log them off (Ctrl, alt, delete, enter to lock or Windows Key + L).
- If you make a data breach by accident, inform Neil as soon as possible.
- If you become aware of a data breach, inform Neil as soon as possible.
- Neil will record the Data Breach and undertake a risk assessment, with Neil/Chris W.
- Neil/Aey will inform the Data subject(s) of the breach and actions taken to reduce any risks.
- Neil/Aey will complete the PDPA Data Breach Notification Form, and report to the Headmaster/School Director.

Appendix C

PDPA Reminders for display

PDPA Data Breach Notification FORM