4.10 Confidentiality Policy
(EYFS & KS1-3)

Reviewer responsible:	**Head of Finance**	Date of last review:	**01/26**
Reviewed by:	**AB/MS**	Date of next review:	**01/27**
Authorised by:	**Exec**		

Notting Hill Prep School, 95 Lancaster Road, London W11 1QQ
020 7221 0727 admin@nottinghillprep.com
nottinghillprep.com

1. Policy owner, approval and review

- Owner: Head (or nominated SLT lead)
- Safeguarding lead: Designated Safeguarding Lead (DSL)
- Data protection lead: DPO / Data Protection Lead
- Approval: Proprietor / Governing Body
- Review: Annually and following any material change in statutory guidance or school practice.

2. Purpose and scope

Notting Hill Prep recognises the importance of confidentiality in building trust with pupils, parents and staff, and in protecting the welfare, wellbeing and safety of our school community.
This policy applies to all staff (teaching and support), volunteers, proprietors/governors, contractors, visiting professionals and agency staff across all school sites.

3. Core principles

We will:

- respect privacy and keep information confidential where appropriate;
- share information only on a "need to know" basis and in line with our professional duties;
- store and handle information securely; and
- maintain accurate and appropriate records.

Confidentiality is not absolute. Information will be shared where necessary to safeguard and promote the welfare of children, to prevent serious harm, or where the law requires disclosure.

4. Aims

- to protect the child at all times and to give all staff involved clear, unambiguous guidance on confidentiality;
- to ensure pupils and parents understand the boundaries of confidentiality and information sharing;
- to provide clear procedures for receiving, recording and sharing information;
- to ensure staff act consistently, proportionately and professionally in all matters of confidentiality.

5. Definitions

Confidential information includes (but is not limited to) safeguarding concerns, pupil welfare information, medical/SEND information, family circumstances, staff HR matters, complaints, and any personal data not intended for public disclosure.

6. Expectations for all staff and volunteers

All adults working in or for the school must:

- treat information learned through their role as confidential;
- discuss pupils and families only with colleagues who genuinely need the information to fulfil their role;
- avoid discussing confidential matters in public areas or social settings;
- seek guidance where unsure.

If in doubt, staff must consult the DSL (or deputy DSL) promptly and must not delay safeguarding action due to uncertainty about confidentiality.

7. Safeguarding and child protection

7.1 What staff must tell pupils
Staff must never promise "total confidentiality" to a pupil. If a pupil discloses something that indicates risk of harm, staff will explain that information must be shared with the DSL (or deputy DSL) to keep them safe, and will be shared only with those who need to know.

7.2 Reporting concerns
Any safeguarding concern or disclosure must be reported immediately to the DSL (or deputy DSL) in line with the school's Safeguarding & Child Protection Policy.

7.3 Information sharing (including without consent)
Data protection law does not prevent information sharing where it is necessary to protect a child from harm; it provides a framework to share information lawfully, proportionately and securely.

Where possible, the school will be open and honest with the child and/or parents about what will be shared, with whom and why. However, we are not required to inform parents/carers if doing so may increase the risk of harm, prejudice an investigation, or place someone at risk.

7.4 Safeguarding records
Child protection/safeguarding records will be kept securely, with access restricted to the DSL team and authorised leaders, and will be managed in line with statutory guidance on child protection files.

8. Working with parents and pupils

We believe it is essential to work in partnership with parents. The school will usually keep parents informed about matters affecting their child's welfare, wellbeing, progress and behaviour.

There will be occasions when information is not shared immediately with parents to safeguard the welfare and wellbeing of the pupil or to follow advice from children's social care/the police.
Where a pupil shares a difficult personal matter, the pupil will be supported and encouraged (as appropriate) to speak with parents/carers, but the school will not place a child at risk by insisting on this.

9. Health professionals and pastoral confidentiality

School nurses and other registered health professionals follow their own professional standards. They may provide confidential support to pupils in line with their codes of practice.

Health information may be shared without consent where there is a safeguarding/public protection justification, or where necessary to protect health, safety or wellbeing.

10. Secure handling of information

Minimum expectations for secure handling:

- use only approved school systems/accounts for storing and sharing confidential information;
- do not use personal email, personal cloud storage, or messaging apps for confidential school business;
- check recipients before sending email; use BCC for parent group emails where appropriate;
- keep paper records secure (locked storage/clear desk) and dispose of confidential waste appropriately;

- store safeguarding/child protection information with restricted access as set out by the DSL.

11. Photographs, video and social media

Parents are reminded that photographs/videos taken at school events may include other children. The school expects parents to act responsibly and respectfully, in line with the school's photography guidance and any permissions/consents in place.

12. Access to records and data protection

Parents (and pupils where appropriate) may request access to personal data via a Subject Access Request. Disclosure will be managed in line with data protection law and may involve redaction/withholding where lawful (for example, to protect third-party personal data or where an exemption applies).

Staff must not release pupil, parent or staff information to third parties (including separated parents, solicitors, or the media) without authorisation from the Head/DPO (and DSL where safeguarding related).

13. Complaints confidentiality

Correspondence, statements and records relating to individual complaints will be kept confidential except where disclosure is required by law, including where required by the Secretary of State or a body conducting an inspection.

14. Breaches of confidentiality and data breaches

A breach includes (but is not limited to) mis-sent emails, lost paperwork/devices, unauthorised access, or inappropriate disclosure.

Any suspected or actual breach must be reported immediately to the Head and the DPO/Data Protection Lead (and to the DSL where a safeguarding record is involved). The school will record, assess and respond in line with its breach management procedures and legal obligations.

15. Training and awareness

Confidentiality and information-sharing expectations form part of induction and are refreshed at least annually, including safeguarding information-sharing and secure handling of records.

16. Non-compliance

Failure to follow this policy may result in disciplinary action and may be referred to external agencies/professional bodies where appropriate.

LINKS TO OTHER SCHOOL POLICIES AND PROCEDURES

This policy is intended to be used in conjunction with the following policies:

- Safeguarding & Child Protection Policy
- Data Protection Policy
- Policy for Education for Ethnic Diversity

- Staff IT Acceptable Use Policy
- Managing Allegations Against Staff Policy

Appendix A: Confidentiality Agreement (for staff/volunteers/contractors)

Confidentiality Agreement - Notting Hill Prep

I understand that in the course of my work at Notting Hill Prep I may have access to confidential information relating to pupils, parents and/or staff. I agree that I will:

- 1) Share information only on a need-to-know basis and only for legitimate school purposes.
- 2) Report any safeguarding concern immediately to the DSL (or deputy DSL).
- 3) Never promise pupils absolute confidentiality and will explain that concerns may need to be shared to keep them safe.
- 4) Handle information securely (approved systems only; no personal email; careful use of email/printing; secure disposal).
- 5) Report any suspected/actual confidentiality or data breach immediately to the Head/DPO (and DSL if safeguarding-related).
- 6) Maintain professionalism and discretion, including outside the workplace and on social media.

Name: _____ Role: _____

Signature: _____ Date: _____