

SCHOOL DATA PROTECTION NOTICE (PRIVACY POLICY)

WHO WE ARE

Downe House School ("the School") is a company limited by guarantee, registration number 2645228 and a charity with a registration number of 1015059. For day-to-day communications, the School is referred to as Downe House.

The School is a Data Controller for the purposes of Data Protection Law¹ which means it determines how an individual's personal data is processed and for what purposes.

WHAT THIS POLICY IS FOR

This policy is intended to provide information about how the School will use (or "process") personal data about individuals including: its personnel², its current, past and prospective pupils, their parents, carers or guardians (referred to in this policy as "parents") and donors.

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. School personnel, parents and pupils are all encouraged to read this Privacy Notice and understand the School's obligations to its entire community.

This Privacy Notice applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form. It applies to offline and online processing, including our websites, portals, applications and IT systems.

This Privacy Notice also applies in addition to the School's other relevant terms and conditions and policies, including, but not limited to:

- any contract between the School and its personnel or the parents of pupils;
- the School's policy on taking, storing and using images or biometric data of pupils;
- the School's policy on the use of CCTV and related security systems;
- the School's safeguarding and pastoral policies;
- the School's Health and Safety policy, including how concerns or incidents are recorded;
- the School's IT policies, including the Information Systems (IS) Acceptable Use policy and e-Safety policy

Anyone who works for, or acts on behalf of, the School (including school personnel, volunteers, governors and service providers) should also be aware of and comply with this Privacy Notice and the School's Data Protection policy, which also provides further information about how personal data about those individuals will be used.

¹ The UK GDPR, the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronic Communications Regulations 2003 (PECR), as amended by the Data (Use and Access) Act 2025 (DUAA).

² School personnel includes employed staff (current, past and prospective), self-employed persons, volunteers, governors and other members of our community.

RESPONSIBILITY FOR DATA PROTECTION

The School has appointed Director of Finance and Operations who, in conjunction with the Headmistress and Director of Digital Delivery and Innovation, will deal with all requests and enquiries concerning the School's uses of individuals personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law. Requests and enquiries should be sent to dataprotection@downehouse.net

DATA WE COLLECT

Depending on the relationship and context, we may process:

- Identification and contact data (e.g., name, date of birth, addresses, email, phone).
- Education records: admissions data, attendance, assessments, exam results, behaviour, SEN.
- Pastoral/safeguarding information and records.
- Financial/billing data (e.g., fee payments, bursary details).
- Employment/HR data (for personnel and applicants).
- Health data (including medical/ dietary/ accessibility needs); religion (for chaplaincy/spiritual care); ethnicity (for statutory monitoring).
- Photographs, audio/video, CCTV/Access control, device/usage logs.
- Biometric identifiers used for specific services (with appropriate consent where required).
- Online identifiers and cookie data.

The sources of this data may be:

- Provided directly by you or your child (forms, portals, correspondence).
- Observed (CCTV, IT logs, class assessments).
- Created by us (reports, results).
- Received from third parties (previous schools, referees, health or safeguarding professionals, exam boards) or public sources (e.g., Companies House, open registers) where lawful.

WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

In order to carry out its ordinary duties to its personnel, pupils and parents, the School may process a wide range of personal data about individuals (including current, past and prospective personnel, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its personnel, or parents of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

Where we rely on legitimate interests, we conduct a Legitimate Interests Assessment (LIA). Recognised legitimate interests includes safeguarding, public security, crime prevention, emergency response and intra-group transmission for internal administration. Where we rely on Recognised Legitimate Interests, a separate balancing test is not required; we still apply necessity and proportionality and meet transparency duties. The School expects that the following uses may fall within that category of its (or its community's) "legitimate interests":

Purpose	Lawful basis	Key data	Typical recipients
Admissions & identity verification	Contract (pre-contract steps); Legitimate Interests (LI)	Identity, prior school records	Previous schools; referees
Delivering education & co/extra-curricular activities	Contract; LI	Education records, pastoral notes	Exam boards; trip organisers
Pastoral care & safeguarding	Legal obligation; Vital interests; Recognised LI (safeguarding/crime prevention/emergency response)	Health, safeguarding, behaviour	Local authority/ Children's Services; Police; NHS
Special Educational Needs (SEN)	Legal obligation; Public task; Explicit consent (where required)	Health/SEN	Local authority; specialists
Fee billing & finance	Contract; Legal obligation (tax)	Contact, financial	Banks; HMRC; auditors
HR & recruitment	Contract; Legal obligation; LI	HR records; DBS; references	DBS; previous employers
IT & network security; filtering/monitoring	LI; Recognised LI (network/information security)	IT logs, device identifiers	IT providers; security vendors
CCTV & site security	LI; Recognised LI (public security/crime prevention)	Images; access logs	Police (where lawful)
Alumnae relations & events	LI; Consent (where required)	Contact, history	Event/venue providers
Fundraising/Development	LI; PECR; Consent for certain channels	Contact, publicly available profile information	Screening partners; payment providers
Direct marketing (school news/events)	LI (with PECR rules); Consent where required	Contact	Email/SMS/social media platforms
Statutory reporting & compliance	Legal obligation	Various	DfE/Ofsted/Exam boards/Local Authority

The School may need to process special category personal data (concerning health, ethnicity, religion, or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so: for example for medical advice, social services, insurance purposes or to organisers of School trips;
- To provide educational services in the context of any special educational needs of a pupil;

- To provide spiritual education in the context of any religious beliefs;
- In connection with employment of its personnel, for example DBS checks, welfare or pension plans;
- To run any of its security systems that operate on personal data, such as for security and other forms of pupil identification (ID Cards, door entry, CCTV, etc.);
- As part of any school or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health, or safeguarding elements; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

We share personal data only where lawful and necessary, typically with:

- Education bodies (DfE, Ofsted/ISI, exam boards), local authorities, police/children's services (safeguarding).
- Health & pastoral professionals (School Nurses/GPs/therapists) as needed for pupil welfare.
- Service providers / processors (MIS/IT hosting, email, filtering/monitoring, cloud storage, messaging, web, analytics, payment and trip providers), under written contracts with appropriate safeguards.
- Professional advisers (legal, audit, insurance), banking and payment services, and fundraising partners for due diligence and screening using publicly available sources.

We assess and contractually bind processors to handle data only on our instructions, with appropriate security and confidentiality including DUAA compatible contractual safeguards.

We may share personal data with The Keepers and Governors of the Possessions, Revenues and Goods of the Free Grammar School of John Lyon within the Town of Harrow-on-the-Hill (the "Corporation"), this being the charitable entity which the School forms part of. Personal data may be shared where necessary to support the governance, management and operation of the School and its relationship with the Corporation, including, for example, for educational and co-curricular activities, regulatory compliance, fundraising and development, and other collaborative activities or shared services. Depending on the purpose of the sharing, the School and the Corporation may act as independent controllers or joint controllers of your personal data.

Occasionally, the School will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority).

For the most part, personal data collected by the School will remain within the School and will be processed by appropriate individuals only in accordance with access protocols. Particularly strict rules of access apply in the context of:

- medical records held and accessed only by the School Nurses and appropriate personnel under the authorisation of the Nurse Manager, or otherwise in accordance with express consent.
- safeguarding files

However, a certain amount of any medical, pastoral and Special Educational Needs (SEN) pupil's relevant information, will need to be provided to personnel more widely in the context of providing the necessary care and education that the pupil requires.

Personnel, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including [Keeping Children Safe in Education](#)) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they

meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as Social Services or police. For further information about this, please view the School's Safeguarding Policies³.

For the purposes of maintaining a safe and secure environment, the School reserves the right to monitor all internet and email traffic through its filtering systems and all domain joined devices through e-Safe monitoring software and services.

Finally, in accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers, cloud storage and social media providers⁴. Where possible this is subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

INTERNATIONAL TRANSFERS

Some processors or sub-processors may be based outside the UK. We will:

- Use adequacy decisions where available; or
- Put in place appropriate safeguards and apply DUAA's data protection test that the destination's protections are not materially lower than the UK's, documenting our assessment.

CHILDREN'S DATA AND THE CHILDREN'S CODE

Where online services we provide are likely to be accessed by pupils, we design them in line with the Age-Appropriate Design Code (Children's Code)—including high-privacy defaults, clear child-friendly information, minimised profiling/geo-location, and DPIAs covering children's risks.

HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary personnel and pupil personnel files is up to 7 years following departure from the School. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. Material will only be kept, if required to do so in law.

Personal data pertaining to prospective personnel and their application process will be removed from the School systems from 2 years.

All School email correspondence is retained for up to 7 years, after which time it is removed from live and archive email systems, along with any personal data contained within.

If individuals have any specific queries about how this policy is applied, or wish to request that personal data, that is no longer believed to be relevant, is considered for erasure, please contact the Director of Finance and Operations dataprotection@downehouse.net. However, please bear in mind that the School may have lawful and necessary reasons to hold on to some data.

COOKIES, ANALYTICS AND SIMILAR TECHNOLOGIES

Our websites and portals may use cookies and similar technologies. We:

- Explain what we use and why;

³ Safeguarding policies comprise: Safeguarding and Child Protection, Keeping Children Safe in Education, e-Safety and Prevent

⁴ Third party terms and conditions apply e.g. X, Facebook, LinkedIn, Google Analytics

- Seek consent for non-essential cookies; and
- Provide a means to withdraw consent at any time.

AUTOMATED DECISION MAKING AND PROFILING

We do not routinely make decisions based solely on automated processing that produce legal or similarly significant effects. If we ever introduce such ADM, we will provide a specific notice explaining the logic involved, significance and the envisaged consequences, and your rights (incl. to obtain human intervention and to contest the decision).

KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The School will use the contact details of parents, alumnae and other members of the School community to keep them updated about the activities of the School, or alumnae and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School may also:

- Share personal data about parents and/or alumnae, as appropriate, with organisations set up to help establish and maintain relationships with the School community, such as the DHS (Downe House Society) which uses legitimate data managed within the Downe House Foundation Office.
- Contact parents and/or alumnae by post and email in order to promote and raise funds for the School and where appropriate, other worthy causes.

As a fundraising organisation, we undertake in-house research and from time to time engage specialist agencies to gather information about you from publicly available sources, for example, Companies House, the Electoral Register, company websites, 'rich lists', social networks such as LinkedIn, political and property registers, and news archives.

We may also carry out wealth screening to fast track the research using our trusted third-party partners. We may also carry out research using publicly available information to identify individuals who may have an affinity to our cause but with whom we are not already in touch. We also use publicly available sources to carry out due diligence on donors in line with the charity's Gift Acceptance Policy and to meet our legal obligations in respect to charity and money laundering regulations.

This research is conducted for our legitimate interests in helping us to understand more about individuals so we can focus conversations we have with them about fundraising and volunteering in the most effective way and ensure that we provide them with an experience as a donor or potential donor which is appropriate.

Should individuals wish to limit or object to any such use, or would like further information about them, please contact the Director of Finance and Operations in writing. Individuals always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School may need nonetheless to retain some personal data (not least to ensure that no more communications are sent to that particular address, email or telephone number).

YOUR RIGHTS

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or for the School to stop processing it, but subject to certain exemptions and limitations.

You have the following rights (subject to legal limits and exemptions):

- Access your data.
- Rectification of inaccuracies.
- Erasure (where applicable).
- Restriction of processing.
- Data portability (for certain data you provided).
- Object to processing (including to direct marketing, and to processing based on legitimate interests).
- Rights relating to automated decision-making/profiling.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, should put their request in writing to the Director of Finance and Operations at dataprotection@downehouse.net. We will respond within one month. If your request is unclear or complex, we may pause (“stop the clock”) while we seek clarification.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information. The School will be better able to respond quickly to smaller, targeted requests for information.

Individuals should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts, nor any confidential reference given by the School for the purposes of the education, training or employment of any individual.

Pupils, where supported by their parents, can make subject access requests for their own personal data. Indeed, while a person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child’s at law. A pupil of any age may ask a parent or other legal representative to make a subject access request on her behalf, and moreover (if of sufficient age) their consent or authority may need to be sought by the parent. Pupils aged 13+ are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Pupils younger than 13 may be sufficiently mature to have a say in this decision. All subject access requests from pupils will therefore be considered on a case-by-case basis.

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the School may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation has been requested).

WHOSE RIGHTS

The rights under Data Protection Law belong to the individual to whom the data relates. However, the School will often rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question, and the pupil’s age and understanding, it is more appropriate to rely on the pupil’s consent.

Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents’ rights at law or under their contract, and all the circumstances.

In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of personnel and expressly withholds their agreement to their personal data being disclosed to their parents, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Personnel and pupils are required to respect the personal data and privacy of others, and to comply with the School's relevant policies, e.g. IS Acceptable Use Policy and the School rules.

DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the School at least on an annual basis of any changes to information held about them. Responsibility for changes in information relating to pupils, rests with the parent.

An individual has the right to request that any inaccurate or out-of-date information about them is erased or corrected (subject to certain exemptions and limitations under the Act): please see above.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to School systems. The use of unauthorised recording technology (e.g. Smart Glasses, Bodycams) is strictly forbidden. All School personnel will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

We implement appropriate technical and organisational measures, including access controls, encryption in transit and at rest (where appropriate), user authentication (e.g., MFA on administrator accounts), vendor due diligence, staff training, secure configuration, and incident/breach response procedures aligned to UK GDPR/PECR.

If a personal data breach occurs, we assess impact and notify the ICO within 72 hours where required, and affected individuals where the risk is high. For PECR-covered communications service breaches, the 72-hour window also applies.

QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the Director of Finance and Operations using the email address: dataprotection@downehouse.net

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should raise a complaint using the email address above. All complaints will be acknowledged within 30 days, investigated and the outcomes communicated without undue delay. Existing parents may use the Complaints Policy and Procedure for Current Parents for concerns not related to Data Protection. The School can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator.

Supervisory authority: Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel: 0303 123 1113.

Revision History:

Revision	Date	Description of changes	Requested By
	May 2018	Implemented	David McClymont
	October 2018	Amendment to the 'How Long We Keep Personal Data' section	Emma McKendrick
	May 2019	Reviewed	David McClymont
	May 2020	Reviewed	David McClymont
	May 2021	Reviewed	David McClymont
	May 2022	Reviewed	David McClymont
	May 2023	Amendment to Keeping in Touch and Supporting the School	David McClymont
	March 2024	Replace DDDI with DFO. Addition of reference to biometric data.	Cliff Kurn
	March 2025	Minor reference updates	Cliff Kurn
	September 2026	Amended to comply with DUAA legislation.	Cliff Kurn

Review Leader: Director of Digital Delivery and Innovation
Reviewed: September 2026
Next Review: September 2027