HEATHSIDE SCHOOL
HAMPSTEAD

GDPR (DATA PROTECTION) POLICY

Introduction

Heathside School has always had a very comprehensive data protection policy and considers protecting your privacy and safeguarding your personal data an utmost priority. The GDPR (General Data Protection Regulations) legislation that was enacted in the UK in 2018 is a further enhancement of previous data protection laws that existed prior to this. Data protection laws govern how schools, authorities, businesses and other organisations process your personal data.

One key guideline is the policies and procedures regarding data protection need to be in plain English and transparent. This policy aims to be as clear as possible and avoid any unnecessary 'legalese' or technical jargon. Heathside is totally transparent about what personal data is collected and how and why it is used.

All schools routinely need to keep and maintain personal and private data in order to carry out normal day to day operations. The overarching reason schools keep this data is to ensure the safety and wellbeing of all pupils, staff and visitors at the school.

We never permit any personally identifiable data to be passed on any third parties to use for any marketing purposes or other unauthorised or unintended purposes. The only times any limited amounts of personal data are ever passed on, is to future/past schools/colleges/employers for references and reports, and to local authorities or government departments for official or legislative reasons.

We ensure that any Personal Data MUST**:**

- be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- be adequate, relevant and not excessive for those purposes;
- be accurate and kept up to date;
- not be kept for longer than is necessary;
- be processed in accordance with the data subject's rights;
- be kept safe from unauthorised access, accidental loss or destruction;
- not be transferred to another country or territory, unless that country has equivalent levels of protection for personal data.

For a school, the following are considered legitimate and lawful reasons to hold and process personal data:

- support the teaching and learning of pupils;
- monitor and report on the progress of pupils;
- support the safeguarding of our pupils and staff;
- provide appropriate pastoral care;

- provide references;
- assess how well the School as a whole is doing;
- communicate with former families/pupils;
- where appropriate, promote the School to prospective pupils (including through the School's website);
- log internet/intranet usage;
- for crime prevention and security purposes, such as CCTV;
- and undertake other reasonable purposes relating to the operation of the School.
- routine vetting and background checks of staff

Terms used in the policy

As the School is responsible for collecting and maintaining private and personal data, we are considered a *'Data Controller'*. This effectively means we are the custodian of any personal data you have provided to us.

The *'Data Subjects'* are the entities the personal data refers to. In the case of a school, these could be Parents, Students, Staff, Volunteers and Visitors etc. Data Subjects have a right to ask for personal data held on them, request that incorrect personal data is corrected, and (where there is no conflict with other regulatory commitments) Data Subjects can also request for certain personal data we hold on them to removed. The procedure to perform any of these actions can be started by making a *'Subject Access Request'.*

The school uses various software systems and services to store, maintain, process and access this data. The providers of these services are called *'Data Processors'*. Any data processors used by the school have issued statements/clarifications and updated their policies in 2018 to reaffirm that they are fully compliant with the GDPR legislation and guidelines. Any personal data is only ever held and transferred in an encrypted and secure manner to data processors. The Data Processors themselves do not have direct access to any of the personal data. They simply provide systems and infrastructure to allow the school to access, store and process the data.

Data Processors sometimes use *'Sub-Processors'* which are used to process a very limited subset of the data, but their access is even further restricted by design, as the encrypted data they process are generally single transactions which are not in context to the main data records held by the school. For example, a specialist sub-processor may process a single credit card transaction or order, but in doing so they have no access whatsoever to the source of personal data held by the school. Any data transactions are only processed outside of the UK if adequate data protection regulations are in operation in those countries.

Data Security

We are obliged to keep all your personal data safe. All personal data is only ever transmitted in a secure and encrypted manner. We require our relevant staff to use secure passwords and enforce additional safeguards such as two-factor authentication, especially for users with access to particularly sensitive personal data. School networks are filtered, and traffic logged. For particularly sensitive information, further safeguards are taken. Staff and older children using any school systems are required to sign Acceptable Use agreements, before any access can be granted.

The school is responsible for ensuring that any personal data on pupils [or staff], to which they have access, or for which they are responsible, is kept securely, for example:

- Kept in a locked filing cabinet; or
- In a locked drawer;
- If it is computerised, is password protected.
- Computers holding any personal data are kept in suitably secure conditions. Personal data should never be stored in an unencrypted format, either locally, via a network or external storage. Industry standard encryption is mandatory.
- Destroyed securely when no longer required.

Subject consent

In some cases, the School can only process personal data with explicit consent of the individual or his/her designated guardian i.e. parent(s). In the case of a school, for most routine personal data, this is deemed to have been given when the parent or guardian accepts the place by admitting their child to the school. If the data is especially sensitive, further express consents may be sought. Agreement to the School processing some specified classes of personal data is a condition of enrolment or employment for both pupils and staff.

The School recognises that, as a data controller, it has a duty of care to all staff and all pupils. It must therefore make sure that employees and pupils and all those who use the School facilities do not pose a threat or danger to themselves, or other users. Therefore, all prospective staff will be asked to consent to their data being processed when an offer of employment is made. In addition, staff must sign an Acceptable Use Agreement before access is provided to the school systems.

For photography or video images of children, a separate consent form is required from all parents authorising the use of images of their children. Where images are published,

such as on the school website, the children are never named or identified. Please see the school Photography Policy for further information.

Sensitive Personal Data (Staff)

The GDPR sets out a series of conditions before an employer can collect, store, use, disclose or otherwise process sensitive personal data. The normal condition is "To process the data for the purpose of exercising or performing any right or obligation which is conferred or imposed by law."

For school staff, an example would be the completion of Disclosure and Barring Service checks and other necessary vetting. In certain circumstances and for official administrative reasons, some personal data may be passed to other authorities and educational establishments. The Head Teacher has the authority to pass on data to other educational establishments as deemed necessary.

Retention of data

The School will keep some forms of personal information for longer than others. The School may need to keep some aspects of central personnel records indefinitely. This will include information necessary in respect of attendance, discipline, positions held, subjects studied, university applications, exam results, dates of starting / leaving and for staff pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references.

The School regularly undertakes procedures to ensure that personal data is not kept for longer than is necessary for the purpose for which it was originally held.

Data is kept for only as long as required. However, this can vary depending on the type of data. For example, some data is kept for longer periods for regulatory reasons, e.g. Attendance Registers, Admission Registers, Staff Records, Financial/Tax data and Health & Safety records.

Old personal data is of limited use to the school as we won’t be able to update it and maintain its accuracy after the child, parent or staff member has left the school. Therefore, where possible, older data is anonymised and converted to stats when the original details are no longer necessary

Please refer to Appendix B for full details of our data retention policy.

Third parties with whom the School may need to share your personal data

From time to time the School may pass your personal data (including sensitive personal data where appropriate) to third parties, including local authorities, other public

authorities, independent school bodies, health professionals and the School's professional advisers, who will process the data:

- to enable the relevant authorities to monitor the School's performance;
- to compile statistical information (used on an anonymous basis);
- to secure funding for the School (and where relevant, on behalf of individual pupils);
- to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for pupils;
- where specifically requested by pupils and/or their parents or guardians;
- where necessary in connection with learning and extra-curricular activities undertaken by pupils;
- to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
- to obtain appropriate professional advice and insurance for the School;
- where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied;
- where otherwise required by law; and
- otherwise where reasonably necessary for the operation of the School.

Please refer to Appendix C for our full Privacy Statement.

Data Integrity

The school does its level best to ensure the data it holds on parents, children and staff members is kept accurate and up to date.

Parents may update their own contact details directly by using an online form, or may contact the school for us to update data on your behalf. For example if you change address, contact numbers or email addresses.

We backup data routinely and regularly to protect your data from any accidental erasure, or any technical issues.

Staff at the school only have access to any personal data that is of relevance to their role. Any changes to data are logged and can be audited. While some data can be edited/updated, critical data cannot be deleted by staff unless they go via the system administrator. This may happen for example, if it is discovered that a second duplicate data record has been created inadvertently.

Data Visibility

All access to any personal data is granular. Only certain types of data are visible to school staff that need access for their day to day roles. Any additional data is not accessible to staff that don’t have a valid reason to have access to it.

For example, while teaching staff do have access to parents' contact details and child medical information so they can react quickly during an emergency. Teaching staff do not need access to additional data which is not relevant to their role as a teacher. For example, financial data is never accessible to teaching staff.

Similarly, admin staff that do not need access to pupil progress data that is intended for teaching staff, are blocked from access.

Data Breaches

While every reasonable effort is made to ensure your personal data is always kept secure, there always remains a possibility of a data breach. No organisation of any size can ever be totally invulnerable to a data breach.

Some breaches can be simple as leaving a confidential page in the output tray of a printer or photocopier, or an unauthorised person overhearing something confidential, or seeing something on a screen which they should not have been able to see. We minimise the risk of such breaches by ensuring sensitive information is only printed in locked rooms or a security PIN number is entered at the printer/copier to retrieve a printout, when it can be safely retrieved privately.

On very rare occasions we may be made aware of major breaches like online hacking, passwords being compromised, or even viruses on computers or devices. A device or computer being lost or stolen is also something that has to be planned for. Any laptop or device which contains any particularly sensitive information is locally encrypted using BitLocker or FileVault or similar technologies to ensure any salvaged storage medium is totally inaccessible to any third party. Mobile devices which have access to any sensitive or personal data are automatically enrolled in device management which requires additional software to be installed before access to any school data is possible. This allows the school to remotely wipe any school data on any lost or compromised device.

There is also a chance that confidential data may be accidentally sent to the wrong destination, due to an incorrect email address, postal address or phone number. To minimise the risk, externally destined emails may be vetted, and staff are encouraged to use initials or codes in messages when referring to a particular child for example, especially when it is obvious due to context that the destination is already aware of the child's name. If in doubt, staff will follow up with a phone call to the recipient. Most school email is internal and encrypted. Only certain staff are permitted to send any email externally.

Whenever a data breach is detected or reported, we react immediately to ensure the breach goes no further and then assess the impact and extent of the breach. We immediately lock down any affected systems and contact all possibly impacted data subjects to ensure they are aware of the breach and offer any help or advice.

In minor cases, where the impact of the breach was low, a report is made and the incident logged. We revisit this info when updating our policies and procedures so we can learn from the incident and minimise the risk of it recurring.

In more serious cases where personal data may have been stolen or compromised, we will immediately contact the authorities for their assistance. The ICO is the first point of contact regarding this.

Subject Removal

A subject can ask for their personal data to be removed or corrected. While we will of course fully evaluate and consider any such request - depending on our other regulatory commitments it may not be possible to delete all or some of your personal data. For active children and staff there is very little data we can remove, while children are still being educated at the school, or staff are still being employed by the school. However, for former students or staff we can delete any personal data that is no longer required for regulatory reasons. Please note some data has to be kept for several years. E.g. Admissions Registers, Attendance Registers, Health & Safety records, employment references and tax records etc.

Data Destruction

Personal data is erased securely when it is no longer required. In the case of paper copies, cross cut shredders are used for any personal or sensitive data. We use a fully compliant third party for secure disposal of paper records. They provide secure shredding bins at all our school buildings and collect and securely destroy and confidential paper periodically. They provide certificates of destruction.

Any defunct computers or electronic devices are wiped using multi-pass wiping utilities such as DBAN, before disposal or repurposing.

Secure disposal companies are used for particularly sensitive data which provide certification verifying compliant destruction.

Staff are required to only process any personal data on secure storage so that data cannot be accessed in case a computer or device is lost or stolen.

For access to personal data from staff members, or older children’s personal devices, the school has the ability to remotely remove any school related data.

Copying school data

Staff are not permitted to make any unauthorised copies of any personal data. Even printouts, or computer files should never be taken off school premises unless adequate safeguards are in place to ensure the data is strictly limited and only for its intended purpose. E.g. emergency contact details for children going on a school trip.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher or nominated representative.

Contacts

If you have any enquiries in relation to this policy, please contact us. The following email address should be used GDPR@heathsideschoolhampstead.com Any Subject Access Requests or Data Removal or Data Corrections should also be addressed here.

Conclusion

Compliance with GDPR is the responsibility of all members of the school community i.e. pupils, non-teaching and teaching staff. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to the School's facilities being withdrawn, or even in extreme cases, a criminal prosecution.

Best Practices for School Staff

1) Always ensure **Personal** information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Always double check with the Senior Leadership Team if any doubt.
2) Staff should note that unauthorised disclosure is a breach of GDPR and may result in a personal liability for the individual staff member.
3) Staff should be vigilant about preferring the use of “bcc” rather than “cc” when using a group email otherwise confidential email addresses of others may be inadvertently shared.
4) Any papers containing personal data which is deemed to contain sensitive information from teachers and support staff from any department should be deposited in one of the secure shredding bins which the School provides for such purposes. For teachers, this should include all trip documentation as well as draft copies of school reports.
5) Any computer hardware that is either defunct or is being returned e.g. when a member of staff leaves, should be given to one of the IT technicians where the hard drive will either be wiped of all data and then the machine reallocated or if the hardware is faulty then it is physically destroyed in a secure manner.
6) All remote devices (including personal ones) used by staff for work purposes should be secure. This may include smartphones, tablets and laptops or any similar devices. They must be password secured with a security PIN code or passwords and have any encryption methods switched on.
7) If using removable media – e.g. flash drives, external hard drives or CD/DVDs, any personal data must be encrypted or password protected.
8) Any staff accessing any school data from a personal device, is only possible by using our authorised device profiles. This ensures the school can remotely wipe and disable access to any school data, in case your device is ever lost or stolen. Staff are obliged to report any lost/stolen device immediately.
9) Staff must never leave sight of a computer that they are working on without either logging off or locking it so that a password is required to resume access. For school provided laptops, please get into the habit of pressing Windows Button (on keyboard) plus the ‘L’ key simultaneously if you have to leave your desk, to lock the screen and require a password upon your return to the desk.
10) Staff must not be in a situation where incoming email alerts could be projected to a class or audience that they are presenting to. Class teachers should routinely use the ‘Freeze’ option on their Interactive Boards or Screens, if the option is available. Alternatively, staff may prefer to extend their ‘desktops’ so their own monitor is showing a different image than the classroom screen visible to students.
11) Staff must never use removable media such as a USB key that they have found or been given by a third party. Please seek the advice of the system administrator immediately.
12) Staff must not access any school systems from untrusted networks such as internet cafés or open public hotspots. Staff should only ever access the school systems remotely through devices provided by the school or via their own devices which have already been approved by the school and then only via trusted internet connections.
13) Staff must always have passwords for logging on to the school system in general. Passwords should be changed regularly.
14) Care must be taken by staff not to divulge passwords or allow passwords to be seen, or allow their accounts to be used by others once logged in.

15) Personal data should never be processed through any unauthorised cloud applications. The school provides any services which are specifically approved for school use and are fully compliant with the school's security standards. School data should never be stored in any free/home-use 'cloud' services – e.g. DropBox, OneDrive etc. However secure cloud (or secure Virtual Learning Environment) services which have been approved for use by the school are permissible as long as adequate safeguards are in place.
16) In some cases, exam data or other confidential info may be sent by postal services. If sending on removable media (see above), it must be via recorded delivery or courier, or preferably hand delivered by staff if possible.
17) Staff should be aware that any emails which contain personal information that may identify individuals may be considered personal data about that individual and as such this information could be included in a Subject Access Request. Staff should be mindful and restrict information or comments in their emails to those which could be shared in future without any difficulties arising. Anything else should be kept for a telephone or face-to-face conversations.
18) It is always good practice to double check that information is going to the correct e-mail address and with the correct document(s) attached. If via email to a recipient or device not on the school system, it must be fully encrypted. The email must use SSL/TLS/HSTS security. If the information is particularly sensitive, or there are any doubts, then manually encrypt with a password any attachments and communicate the password separately (preferably not by email). Make use of the 'Confidential Mode' provided by the school email systems, which provides additional safeguards for sending confidential emails.
19) When data is being uploaded to an official government website, always double check the connection is secure. If via internet file transfer e.g. FTP or HTTP (web upload), the data must be password protected and encrypted (i.e. HTTPS or SFTP minimum)
20) If a name of a child or staff member has already been implied by previous communication (e.g. face to face or telephone) any further correspondence regarding the person should contain coded references rather than any names, e.g. use initials rather than a full name. If in doubt, always meet or call to avoid any ambiguity or misunderstanding.

Appendix A

HEATHSIDE SCHOOL
HAMPSTEAD

Subject Access/Removal Requests

Data subject access requests can come from employees, parents and pupils (past and present) or from a third party such as the police or CPS. All requests, if received by a member of staff, should be copied to gdpr@heathsideschoolhampstead.com

Data subjects can request copies of any personal data the school holds on them by sending us Subject Access Requests. There is a procedure for verifying the request is bona fide and a dialog is started with the subject to seek any clarifications. We aim to initially respond to a Subject Access Request within 72 hours under normal circumstances. However, it usually takes to up to 30 days to fully comply with a request. In rare circumstances, if a lot of data is involved, or the nature of the request requires data to be redacted, if for example, it is inextricably linked with personal information about other subjects, we may negotiate a longer period with the requestor. Where possible, we will endeavour to provide any data in a portable electronic format.

Please note a Subject Access Request only relates to **personal** information. It is **not** the same as Freedom of Information requests or other disclosure requests, which certain organisations such as public bodies have to adhere to. The school is mindful of all its legal responsibilities but does not have the same obligations as public bodies.

Actioning a subject access request

1. Requests for personal information must be made in writing; which may include email, and be addressed to the Headteacher**.** If the initial request does not clearly identify (e.g. ambiguous, or too vague) the personal information required, then further enquiries will be made.

2. The identity of the requestor must be established and verified before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child (if from a parent). Evidence of identity can be established by requesting production of standard forms of ID (such as):
   - passport
   - driving licence
   - utility bills with the current address
   - Birth / Marriage certificate
   - P45/P60
   - Credit Card or Mortgage statement

3. Any individual has the right of access to personal information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. Conversely, a child with the competency to understand, can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. If the provision of information is straightforward then the school will not charge to provide it. However, if the information provided is overly excessive or repetitive, will require lots of redaction (to avoid any divulging any personal data not related to the subject) the school has the right to charge for reasonable costs incurred.

5. The school will aim to initially respond to subject access requests, once officially received and verified, within 72 hours. We will verify and clarify what information is being asked for and whether there is a legal basis to provide it. If there is any doubt, the school will ask for a face to face meeting to clarify an ambiguity. It may take up to 30 days to fully process the request after the identity and clarifications are provided. Please note that subject access requests sent outside of the school term, e.g. during the holidays, or other times where the school is closed, may be subject to further reasonable delays.

6. The GDPR, and our other regulatory commitments allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure**. For example, if there is legally privileged information regarding a current legal matter, legal advice will be sought before entertaining any Subject Access Request that may prejudice a current case.

7. Third party information is that which has been provided by another party, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent will normally be obtained from where the personal data originated.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are any concerns over the disclosure of any information, then additional advice will always be obtained from the school's legal team.

10. Where redaction (information blacked out/removed) has taken place then a full unredacted copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Personal Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained.

12. Personal information can be provided at the school with a member of staff on hand to help and explain matters if requested or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be employed to ensure secure delivery. In the case of electronic transfer that all information must be encrypted and password protected.

Appendix B

HEATHSIDE SCHOOL
HAMPSTEAD

DATA RETENTION POLICY

This policy has been created in accordance with the Data Protection Act 2018 (General Data Protection Regulation) and good practice advice from the National Independent Bursars Association. This policy provides minimum retention periods for all data held or managed by the college, some of which may be personal data.

Data Retention Periods:

Data Area	Record	Retention Period
COLLEGE-SPECIFIC RECORDS	Registration documents of College	Permanent
	Attendance Register	6 years from last date of entry, then archive.
	Minutes of Governors' meetings	6 years from date of meeting
	Annual curriculum	From end of year: 3 years (or 1 year for other class records: e.g. marks / timetables / assignments)
INDIVIDUAL STUDENT RECORDS	Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if student not admitted, no longer than 1 year from that decision).
	Examination results (external or internal)	7 years from student leaving college
	Student file including: • Student reports • Student performance records	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to

	• Student medical records	potential claims should be kept for the lifetime of the student).
	Special educational needs records (to be risk assessed individually)	35 years from Date of birth (allowing for special extensions to statutory limitation period)
SAFEGUARDING	Policies and procedures (including audits)	Keep a permanent record of historic policies
	DBS disclosure certificates (if held)	12 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
	Accident / Incident reporting	Indefinitely (as recommended by the Goddard inquiry)
	Child Protection files	Indefinitely (as recommended by the Goddard inquiry)
EMPLOYEE / PERSONNEL RECORDS	Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
	Contracts of employment/contract for services/consultancy agreements (self-employed or contracted personal) (offer letters and variation letters)	7 years from effective date of end of contract
	Employee appraisals or reviews	Duration of employment plus 7 years
	Staff personnel file (includes grievances, capability and disciplinary documentation, qualifications,	As above, but do not delete any information which may be relevant to historic safeguarding claims.

	termination documentation, references, training records, parental leave records)	
	Payroll, salary, maternity pay records	6 years
	Pension or other benefit schedule records	Permanent, depending on nature of scheme
	Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
	Immigration records	4 years
	Health records relating to employees	7 years from end of contract of employment
INSURANCE RECORDS	Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
ENVIRONMENTAL, HEALTH & DATA	Accidents to children	25 years from birth (longer for safeguarding – see safeguarding)
	Accident at work records (staff)	4 years from date of accident, but review case-by-case where possible
	Staff use of hazardous substances	7 years from end of date of use
	Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.
	Data protection records documenting processing activity, data breaches	No limit: as long as up-to-date and relevant (as long as no personal data held)

Appendix C

HEATHSIDE SCHOOL
HAMPSTEAD

PRIVACY NOTICE

Heathside School is part of the Dukes Education Group.

Heathside respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our websites (regardless of where you visit them from) and tell you about your privacy rights and how the law protects you.

Summary of how we use your personal data

Heathside uses your personal data:

- where we need to perform the contract which we are about to enter into, or have entered into, with you;
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests;
- where we need to comply with legal obligations;
- where we have your consent.

Personal data is shared with other companies in the Dukes Education Group and on occasion with third parties, such as:

- companies that assist us in performing our services;
- our insurance providers;
- companies carrying out background checks (where relevant and necessary).
- Where we rely on your consent, such as for marketing purposes, you can withdraw this consent at any time.
- Our privacy policy sets out more details of this processing, including details of your data protection rights, including your right to object to certain processing.

What does this policy cover?

This policy describes how Heathside and other companies in the Dukes Education Group will make use of your personal data when you register your details or your child's details on any one of the Dukes Education Group websites, so when we mention "Controller", "we", "us" or "our" in this privacy policy, we are referring to the relevant company in the Dukes Education Group responsible for processing your personal data.

It also describes your data protection rights, including a right to object to some of the processing which a member of the Dukes Education Group carries out. More information about your rights, and how to exercise them, is set out in the "What rights do I have?" section.

What information do we collect?

We collect and process personal data about you when you interact with us and our websites, and when you purchase resources and/or services from us. This includes:

- your name, your child's name, username and password;
- your / your child's gender;
- your age/date of birth and / or your child's age/date of birth together with any relevant medical information required for us to perform a service (only where necessary);
- your home address, email address and phone number;
- your payment and delivery details, including billing address and credit card details,
- where you make purchases from us (where relevant);
- your marketing preferences, including any consents you have given us;
- communications that you may send to us;
- related to the browser or device you use to access our website.

How do we use this information, and what is the legal basis for this use?

We process this personal data for the following purposes:

- To fulfil a contract, or take steps linked to a contract: this is relevant where you purchase resources or services from us. This includes:
    - verifying your identity;
    - taking payments;
    - communicating with you;
    - providing customer services and arranging the delivery or other provision of resources or services.
- As required to conduct our business and pursue our legitimate interests, in particular:
    - we will use your information to provide details of resources and services you have enquired about or resources or services you have requested, and respond to any comments or complaints you may send us;
    - we monitor use of our websites and online services, and use your information to help us monitor, improve and protect our resources, content, services and websites, both online and offline;

- we use information you provide to personalise our website, resources or services for you;
- where relevant, if you provide a credit or debit card as payment, we also use third parties to check the validity of the sort code, account number and card number you submit in order to prevent fraud (see data sharing below);
- we monitor customer accounts to prevent, investigate and/or report fraud, terrorism, misrepresentation, security incidents or crime, in accordance with applicable law;
- we use information you provide to investigate any complaints received from you or from others, about our website or our resources or services;
- we will use personal data in connection with legal claims, compliance, regulatory and investigative purposes as necessary (including disclosure of such information in connection with legal process or litigation), for example we may need to share personal data with the Department of Education or an inspection authority to comply with our regulatory obligations;
- we use personal data of some individuals to invite them to take part in market research. • Where you give us consent:
- we will send you direct marketing in relation to our relevant resources and services, or other resources and services provided by us.;
- we place cookies and use similar technologies in accordance with our cookies policy (see below paragraph *Cookies and how we use them*) and the information provided to you when those technologies are used;
- on other occasions where we ask you for consent, we will use the personal data for the purpose which we explain at that time.

- For purposes which are required by law:
  - where we need parental consent to provide online services to children under 13. However, most of our websites are not designed for children under 16;
  - in response to requests by government or law enforcement authorities conducting an investigation.

Relying on our legitimate interests

We have carried out balancing tests for all the data processing we carry out on the basis of our legitimate interests, which we have described above. You can obtain information on any of our balancing tests by contacting us using the details set out later in this notice.

Withdrawing consent or otherwise objecting to direct marketing

Wherever we rely on your consent, you will always be able to withdraw that consent, although we may have other legal grounds for processing your personal data for other purposes, such as those set out above. In some cases, we are able to send you direct marketing without your consent, where we rely on our legitimate interests. You have an absolute right to opt-out of direct marketing, at any time. You can do this by following the instructions in the communication where this is an electronic message, updating your preferences in any account or by contacting us using the details set out below.

Who will we share this personal data with, where and when?

We will share your personal data within the Dukes Education Group for reporting, safeguarding, quality control and potential referral basis (for example, to our consultancy division in respect of university applications). Personal data will also be shared with other organisations, such as insurers and organisations which conduct background checks, where necessary.

Personal data may be shared with government authorities and/or law enforcement officials if required for the purposes above, if mandated by law or if required for the legal protection of our legitimate interests in compliance with applicable laws.

Personal data will also be shared with third party service providers, who will process it on behalf of a Controller for the purposes identified above. In particular, we use third party providers of website hosting, maintenance and identity checking.

In the event that the business is sold or integrated with another business, your details will be disclosed to our advisers and any prospective purchaser's adviser and will be passed to the new owners of the business.

Cookies and how we use them

Cookies are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Some web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

What rights do I have?

You have the right to **ask us for a copy** of your personal data; to **correct**, **delete** or **restrict** (stop any active) processing of your personal data; and to **obtain the personal data you provide to us for a contract or with your consent in a structured, machine readable format**, and to ask us to **share (port) this personal data with another controller.**

In addition, you can **object to the processing** of your personal data in some circumstances (in particular, where we don't have to process the personal data to meet

a contractual or other legal requirement, or where we are using the personal data for direct marketing).

These **rights may be limited**, for example if fulfilling your request would reveal personal data about another person, where they would infringe the rights of a third party (including our rights) or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping. Relevant exemptions are included in both the GDPR and in the Data Protection Act 2018. We will inform you of relevant exemptions we rely upon when responding to any request you make.

To exercise any of these rights, or to obtain other information, such as a copy of a legitimate interests balancing test, you can get in touch with us via our Data Protection Champion using the details set out below. If you have unresolved concerns, you have the **right to complain** to a data protection authority where you live, work or where you believe a breach may have occurred. This is likely to be the Information Commissioner's Office in the UK.

How long will you retain my personal data?

We only retain your personal data for as long as is required by law, or for as long as necessary for the purposes for which we process your personal data. Please refer to our Data Retention Policy for further information.

How do I get in touch with you?

We hope that we can satisfy queries you may have about the way we process your personal data. If you have any concerns about how we process your personal data, or would like to opt out of direct marketing, you can get in touch with our Data Protection Officer, Andy Mirza at Heathside School Hampstead, 84A Heath Street, London NW3 1DN or by email: gdpr@heathsideschoolhampstead.com

Which Controller entity is my data controller, and which affiliates might my personal data be shared with?

The Controller for your information is the entity with which you have a relationship, or which manages the website you have visited.

A full list of Controllers in the current Dukes Education Group is set out below:

Dukes Education Holdings Limited; DEG Investments Ltd; Dukes Education Finance Ltd; DEG Bidco Ltd; Dukes Education Dukes Education Group Ltd; CSFC Ltd; RIC Trading Ltd; Fine Arts College Ltd; Heathside School Ltd; Sussex Summer Schools Ltd; Summer Boarding Courses Ltd; Dukes Education Ltd; Dukes Guardians Ltd; Dukes Schools Ltd; Minerva Education Holdco Ltd; Minerva Education Finance Ltd; Eaton Square Schools Limited; Eaton Square Kensington Limited; Sancton Wood School Ltd; The Hannay-Rowe Education Company Ltd; Knightsbridge School Limited; Miss Daisy's Schools Ltd; Little Owls School Limited.