Hampton Court House

Data Protection and Privacy Policy

Last Updated: September 2026

Next Review: August 2027

Reviewed by AMI

Introduction

Hampton Court House School (hereinafter HCH or The 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. Further amendments which affect GDPR were made by Data (Use and Access) Act 2025 (the DUAA), and additional amendments and anexes were revised in GDPR in 2026.

Data protection legislation governs 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 language and fully transparent. This policy aims to be as clear as possible and avoid any unnecessary 'legalese' or technical jargon. HCH 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 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 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;
- any further legitimate interests, detailed in Annex 1 of GDPR
- Other legitimate reasons such as crime prevention, emergency response, safeguarding, and public body requests

Under 'standard legitimate interests', schools weigh the processing needs against the rights of individuals. The new 'recognised legitimate interests' removes this requirement for a specific list of purposes set out in a new Annex 1 to the UK GDPR:

- Safeguarding national security
- Protecting public security and defence
- Responding to emergencies
- Investigating crime
- Safeguarding vulnerable individuals
- Disclosures to public bodies carrying out public tasks

Automated Decision-Making (ADM): We may on rare occasions have legitimate interests for solely automated decision-making (if no special category data is involved), provided individuals can contest decisions.

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 the 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 *'Data Subject Access Request' (DSAR).*

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 and aligned 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. In all cases this is only permitted if the country of the (sub)processor has been deemed to have data protection laws and practices that are not materially lower than that of the UK. If there is any doubt about the adequacy of international data transfers, we will refer to ICO guidance and use their 'Data Protection Test'.

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 digital, is password protected or encrypted.
- 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.
- Data Centres holding any data are suitably secure.
- 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.

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, unless express consent has been given. 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 safe and 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 legitimate 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 by logged in verified users 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 sensitive information is always locally encrypted using BitLocker or FileVault or similar technologies to ensure any salvaged storage medium is totally inaccessible to any third party. Any computers or mobiledevices 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 or lock 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 (within 72 hours).

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 if it 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 ISO certified data disposal company for secure disposal of any paper records. They provide secure shredding bins at all our school buildings and collect and securely destroy any confidential paper periodically. They provide certificates of destruction.

Any defunct computers or electronic devices are fully wiped before disposal or repurposing.

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 any access to any school personal data from computers or mobile 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, which is then safely destroyed after its intended purpose.

Complaints

In all cases, any complaints regarding data protection must be addressed to the School via the Principal or Data Protection Lead (ami@hchnet.co.uk) . We will acknowledge your complaint within 30 days of receiving it as per ICO guidance. Without undue delay we will take appropriate steps to respond to your complaint, including making appropriate enquiries and keep you informed. Furthermore, we will, without undue delay inform you of the outcome of your complaint. If you are not satisfied with the outcome, you have a right to escalate your complaint to the Information Commissioner's Office (ICO). However, if you have not complained to the school first, the ICO will direct you back to the school.

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 Principal or nominated representative.

Contacts

If you have any enquiries in relation to this policy, please contact us. Our Data Protection Lead is Andy Mirza, and can be contacted on ami@hchnet.co.uk 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 device management protocols 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 or have sufficient account protection safeguards in place such as multi-factor authentication.

14) Care must be taken by all users 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/secure Mode' provided by the school email systems, which provides additional safeguards for sending confidential emails, which adds extra safeguards to ensure only the intended recipient can access the information.

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

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 ami@hchnet.co.uk

Data subjects have the right to request copies of any personal data the school holds on them by sending us a Subject Access Request. There is a procedure for verifying the request is bona fide and a dialog is started with the subject to seek any clarifications. The timeline for handling DSARs can be put on hold and effectively the clock stopped, whilst we verify the identity of the subject (or representative) making the request and ascertaining the legitimacy and scope of the request.

We aim to initially acknowledge 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. Please note the school is only obliged to conduct a 'reasonable and proportionate search'.

In some circumstances, if a lot of data is involved, or the nature of the request requires a lot of data to be redacted, (for example, it is inextricably linked with personal information about other subjects, we may mutually negotiate a longer period with the subject. 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 Principal 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 acknowledge subject access requests, once officially received and verified, within 72 hours (working days only). 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

DATA RETENTION POLICY

We keep your information for as long as we need to in order to educate and look after you. We will keep a lot of information after you have left the School, for example, so that we can find out what happened if you make a complaint.

In some cases we may keep your information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under data protection law.

Data Area	Record	Retention Period
SCHOOL-SPECIFIC RECORDS	Registration documents of school/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 school/college
	Student files including: Student reports Student performance records Student medical records	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to 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, termination documentation, references, training records, parental leave records)	As above, but do not delete any information which may be relevant to historic safeguarding claims.

	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

Privacy Notice for Parents

Introduction

This notice is to help you understand **how** and **why** Hampton Court House School (the **School**, 'we') collect personal data about you and your children and **what** we do with that information. It also explains the decisions that you can make about your information.

If you have any questions about this notice please contact the Data Protection Lead.

What is "personal data"?

Personal data is information that is about you and from which you can be identified.

This includes your contact details, next of kin and financial information. CCTV images, photos and video recordings of you are also personal data.

Where we get your personal data from and who we share it with

We obtain your personal data from a number of different sources. We get a lot of information from you (eg, when you complete the application form). We also get information from other sources such as our teachers, your child, your child's previous schools, other members of your family, other pupils and their parents, as well as from people outside of the School such as the local authority.

We will also share information with these people and organisations where appropriate. For example, if you tell us about something that has happened at home, we will share this with your child's teachers if relevant.

The sections below contain further information about where we get your personal data from and with whom it is shared.

The purposes for which we use your information and the lawful bases

We use your information in order to:

1. Carry out our obligations and enforce our rights under our contract with you;
2. Teach your child and our other pupils;
3. Look after your child and others such as other pupils;
4. Enable the School to comply with its legal obligations, to assist the School regarding the management and operation of the School and to advance and protect the School's interests, objects and reputation; and
5. Fundraise, market and promote the School. For example, by using photographs in the School prospectus, on the School's website or in social media.

Our lawful bases for using your personal data are as follows:

- **Contract:** We will need to use your information in order to perform our obligations under our contract with you and for you to perform your obligations as well. For example, we need your name and contact details so that we can update you on your child's progress and so that we can contact you if there is a concern. We may also rely on this basis where you have asked

us to do something before entering into a contract with us.

- **Legitimate interests:** This means that the School is using your personal data where this is necessary for the School's legitimate interests or someone else's legitimate interests. Specifically, the School has a legitimate interest in educating and looking after its pupils, complying with its agreement with you for your child to be at the School, making sure that we are able to enforce our rights against you, for example, so that we can contact you if unpaid school fees are due, investigating if something has gone wrong and protecting promoting and improving the School. This basis applies to all of the 5 purposes listed above.

- **Public task:** This allows the School to use personal data where doing so is necessary in order to perform a task in the public interest. This basis applies to purposes 2, 3 and 4 above. For example, we are performing a task in the public interest when we teach and look after your child.

- **Legal obligation:** The School might need to use your information in order to comply with a legal obligation, for example, to report a concern about your child's wellbeing to Children's Services or in relation to inspections. Occasionally we may have a legal obligation to share your personal data with third parties such as the courts, local authorities or the police. More detail of when we will do so is set out below.

- **Vital interests:** In limited circumstances we may use your information to protect your vital interests or the vital interests of someone else. For example, to prevent someone from being seriously harmed.

The section below contains more information about our purposes for using your personal data and the lawful bases.

Our purposes and lawful bases in more detail

This section contains more detail about the purposes for which your personal data is used, the applicable lawful bases as well as further information about sources and recipients. It does not say anything different to what's set out above but goes into a lot more detail.

We have also used a colour code system so that you can see which bases we are relying on for each of the purposes described at paragraphs 1 to 43 below. LI means legitimate interests, CT means contract, PI means public task, LO means legal obligation and VI means vital interests. So if we have (LI, PI) that means we are relying on both legitimate interests and public task for that purpose.

1 The School's primary reason for using your personal data is to provide educational and pastoral services to your child (LI, CT, PI).

2 We will use information about you in order to process your application for your child's admission to the School. We obtain information about you from the admissions forms and from your child's previous schools. We also may get information from professionals such as doctors and local authorities (LI, CT , PI).

3 We will have information about any family circumstances which might affect your child's welfare or happiness. This is to help us provide appropriate care and support to your child (LI, CT, PI).

4 We will need information about any court orders or criminal petitions which relate to you. This is so that we can safeguard the welfare and wellbeing of your child and the other pupils at the School (LI, CT, PI).

5 We use CCTV to make sure the school site is safe. Images captured of you via CCTV will be your personal data. CCTV is not used in private areas such as toilets or changing rooms (LI, CT, PI).

6 We will use your personal data to take other steps to make sure the school site and buildings are safe, for example, we keep a record of visitors to the school site at any given time] (LI, PI, LO).

7 If there is a complaint or grievance made to the School that involves you then we will use your information in connection with that complaint or grievance (LI, PI).

8 The School may share information about you with the local authority for the purpose of the preparation, implementation and / or review of your child's Statement of Special Educational Needs or Education Health and Care Plan (LI, PI, LO).

9 Where appropriate, the School will have information about your religious or other beliefs and practices. For example, if you do not eat certain foods (LI, PI).

10 We may take photographs or videos of you at School events to use on social media and on the School website. This is to show prospective parents and pupils what we do here and to advertise the School. We may continue to use these photographs and videos after your child has left the School (LI).

11 We will send you information to keep you up to date with what is happening at the School or the wider group of school's and companies to which the school belongs (the Dukes Education Group). For example, by sending you information about events and activities taking place across the school or the wider Dukes Education Group and the School newsletter (LI).

12 We will keep details of your address when your child leaves the School so we can find out how your child is progressing. (LI).

13 Where required, appropriate or necessary, we will pass on your details to our parent companies and / or other education establishments who are members of the Dukes Education Group (see www.dukeseducation.com) (LI).

14 We may use your information when ensuring network and information security, for example, our anti-virus software might scan files containing information about you (LI).

15 We also keep some information indefinitely for archiving purposes (this is known as "archiving in the public interest" under data protection law) and for historical research purposes. This includes the School's legitimate interest in research; supporting long- term accountability; enabling the discovery and availability of the School and the wider school community's identity, memory, culture and history; enabling the establishment and maintenance of rights and obligations and of precedent decisions; educational purposes; and commercial and non-commercial re-use. For example, we keep some old photographs so that we have a record of what the School was like in the past. Information held in our archive may be made publicly available but this would only be done in compliance with data protection laws (LI, PI).

16 We may use your information in connection with legal disputes (LI, PI, LO).

Financial information

17 We will process financial information about you in relation to the payment of fees. In some cases we get information about you from third parties such as credit reference agencies or from your child's previous school(s) (LI, CT).

18 We will hold information about bankruptcy petitions and statutory demands, where relevant (LI, CT).

19 We may search the files of any licensed credit reference agency in order to verify your identity. This also allows us to assess your application for the award of a bursary or for credit in contemplation of an agreement for the deferment of fees. The credit reference agency will keep a record of that search and details about your application. This record will be seen by other organisations which make searches about you (LI, CT).

20 We may share your information with debt recovery suppliers if you do not pay any school fees owed to the School (LI, CT).

21 We will obtain information about you from publicly available sources, such as (by way of example only) Companies House, Experian (or other credit reference agencies) or Zoopla, to assess your ability to pay School fees (LI, CT).

Sharing personal data with others

22 In accordance with our legal obligations, we will share information with local authorities, the Independent Schools Inspectorate / Ofsted and the Department for Education, for example, where we have any safeguarding concerns or to comply with our legal obligations. These organisations may also provide information to us for these purposes (LI, LO, PI).

23 On occasion, we may need to share your information with the police for the prevention and investigation of crime or the apprehension or prosecution of offenders. We will only do this in specific circumstances to assist the police with their investigations (LI, CT, LO, PI).

24 We may need to share information about you with the Health and Safety Executive

(a government organisation) if there is a health and safety issue at the School (LI, LO, PI).

25 In certain circumstances, we may also need to share information with our legal advisers for the purpose of obtaining legal advice (LI, LO, PI).

26 Occasionally we may use consultants, experts and other advisors to assist the School in fulfilling its obligations and to help run the School properly (e.g. our accountants). We will share your information with them if this is relevant to their work (LI, CT, PI).

27 If your child is not of a British or Irish nationality citizen we have to make sure that your child has the right to study in the UK. Sometimes the government will ask us to provide information as part of our reporting requirements. In addition to this we have a duty to provide information about you to UK Visas and Immigration to comply with our duties as a Child Student / Student sponsor under the Points Based Immigration System (LI, CT, LO, PI

28 We may share some information with our insurance company to make sure that we have the insurance cover that we need or in connection with an actual or possible claim (LI, PI).

29 If the School is dealing with a request for information, query, complaint or grievance (e.g. from another parent), we may need to share your information with other parties if it is relevant and appropriate to do so. For example, with the appropriate staff, pupil or parent involved and governors (LI, PI)

30 If you have unpaid fees we may share information about this with other schools or educational establishments to which you intend to send your child (LI).

31 If your child leaves us to attend another school we may provide that school with information about you. For example, details of family circumstances if there have been any safeguarding incidents (LI, LO, PI).

32 We may share information about you with others in your family, such as another parent or step-parent. For example, where this is part of our obligation to take care of your child, as part of our wider legal and regulatory obligations, or in connection with school fees (LI, PI).

33 We may need to share information if there is an emergency, for example, if you are hurt whilst on School premises (LI, VI).

34 We will share information about you with the other schools or companies in the Dukes Education Group. For example, financial information or details of family circumstances (LI, PI).

35 If you have appointed an agent to act on your behalf, we may share information with them. For example, we may send letters to them so that they can pass these on to you (LI).

36 If you have appointed an educational guardian (and/or there are homestay arrangements) for your child, we may share information with them. For example, academic, medical and behavioural information regarding your child (LI).

37 We may send you information about the School before you accept a place for your child. For example, we may send you a copy of the school prospectus (LI).

38 If your child has a Statement of Special Educational Needs or an Education and Health Care Plan (**EHCP**), we will share information with and obtain information from the local authority about you (LO, PI).

39 If ever in the future, we are considering restructuring or selling our business we may share your information with the other parties involved and with the relevant professional advisors (LI). Some of the records the School keeps and which contain your personal data may be used by the School (or by someone else such as the government) to check that the School has been a good school (LI, PI).

40 The School must make sure that our computer systems are working well and are secure. This may involve information about your child, for example, our anti-virus software might scan files containing information about your child (LI).

41 We will share your personal data with Governors and the owners of the School if it concerns something that the School needs tell them about for the purposes set out in this notice, including to enable them to exercise their functions and fulfil their

duties as School Governors. For example, if there is a concern involving you or your child or something which affects the running of the School (LI, PI).

As you will see from the above, in some cases we will rely on more than one lawful basis above for a particular use of your information. In addition, we may move from one of the lawful bases listed above to another as circumstances change. For example, as a safeguarding matter becomes more serious, we may start to rely on legal obligation to share personal data with the local authority in addition to the other lawful bases which are noted for safeguarding purposes.

We may use third parties to handle personal data on our behalf for the following purposes:

- IT consultants who might access information about you when checking the security of our IT network;
- we use software, apps and websites to help us with teaching, and to help us provide pastoral support to our pupils. For example, we may use an app which allows pupils to access homework which has been set by their teachers; and
- we use third party "cloud computing" services to store some information rather than the information being stored on hard drives located on the School site.

If you have any questions about any of the above, please speak to the Data Protection Lead.

More sensitive types of personal data

The School has extra obligations in relation to some types of more sensitive personal data. This applies to the following categories of information: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic information, biometric information, health information, and information about sex life or orientation and information about criminal convictions or offences. When the School handles these types of information it will usually be doing so because:

- It is in the substantial public interest to do so, for example, to assist the School comply with its safeguarding obligations.
- There will be times when the School needs to use your information because we are an employer (e.g. we employ teachers). Also the School may use your information to comply with social protection law (e.g. to look after your child) and social security laws. Social protection law is concerned with preventing, managing, and overcoming situations that adversely affect people's wellbeing.
- To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.
- It is necessary for the establishment, exercise or defence of legal claims. For example, this allows us to share information with our legal advisors and insurers.

Appendix D

Privacy Notice For Older Pupils

Introduction

This notice is to help you understand **how** and **why** the **School** ('we') collects your personal data and **what** we do with that information. It also explains the decisions that you can make about your personal data.

If you have any questions about this notice please talk to the admissions team.

What is "personal data"?

Personal data is information which is about you.

This includes information such as your name, date of birth and address as well as things like exam results, medical details, unique pupil number and information about how well you behave. CCTV images, photos and video recordings of you are also your personal data.

Where we get your personal data from and who we share it with

We get your personal data from lots of different sources such as your teachers, parents, your old Schools and any future School, other pupils and their parents, as well as from people outside of the School such as the Government.

Sometimes, we will also share information with these people and organisations, for example, we will tell your parents about how well you are doing at School.

Below, we give lots of examples of where we get your information from, and who we share it with.

Why we use your personal data and our lawful bases for doing so

The School needs to use your information in order to:

1. Teach you and other pupils;
2. Look after you and other people such as other pupils;
3. Make sure that you and others are behaving properly;
4. Make sure that the School complies with the law, is well managed and that we protect the School; and
5. Advertise the School and tell people about the School and what we do here e.g. we may use photographs of you in our prospectus, on our website or in social media.

We can only use your personal data if we have a good reason to do so. This is about having a "lawful basis" to use your personal data. Our lawful bases are as follows:

- **Legitimate interests:** This means that the School is using your information where this is necessary for the School's legitimate interests or someone else's legitimate interests. Specific ally, the School has a legitimate interest in educating and looking after its pupils, complying with its agreement with your parents for you to be at the School, promoting and protecting the School and making it better. Legitimate interests only applies where these legitimate interests are not overridden by your interests, rights and freedoms. Legitimate interests applies to all of the 5 purposes listed above.

- **Public task:** This allows the School to use personal data where doing so is necessary in order to perform a task in the public interest. This basis applies to purposes 1, 2, 3 and 4 above. For example, we are performing a task in the public interest when we teach and look after you.

- **Legal obligation:** The School might need to use your information in order to comply with a legal obligation, for example, to report a concern about your wellbeing to Children's Services. Occasionally we may have a legal obligation to share your personal data with third parties such as the court.

- **Vital interests:** Although this won't happen very often, we may need to use your information to protect you or someone else. For example, to prevent someone from being seriously harmed or killed.

The section below contains more information about our purposes for using your personal data and the lawful bases.

Our purposes and lawful bases in more detail

This section gives you a lot more information about why the School uses your personal data, where we get it from and who it is shared with, and which lawful bases apply. It does not say anything different to the sections above but goes into a lot more detail.

We have used a colour code system so that you can see which lawful bases we are relying on for each of the purposes described at paragraphs 1 to 46 below.

The letters highlighted in different colours below refer to the lawful bases. So LI means legitimate interests, PI means public task, LO means lawful obligation and VI means vital interests. So if we have (LI, PI) that means we are relying on both legitimate interests and public task for that purpose.

1 The School's primary reason for using your personal data is to provide you and other pupils with an education (LI, PI).

2 The School will also use your personal data to safeguard and promote your welfare and the welfare of others (for example, so that we can look after you if you are hurt) (LI, PI, VI).

3 We use information about you during the admissions process e.g. when marking your entrance exams and learning more about you from your parents before you join the School. We may let your old School or School know if you have been offered a place at the School as they have a legitimate interest in finding out how what happens to their former pupils as this will help them support their other pupils when they leave the School or School. The admissions forms which your parents complete give us lots of personal data about you such as your name, contact details, disabilities, any particular difficulties you have with work, hobbies and interests, medical information (such as information about an allergy) and family circumstances. We get information from you, your parents, your teachers and other pupils. Your old School also gives us information about how well you did and any difficulties you had so that we can teach and care for you (LI, PI).

4 Sometimes we get information from your doctors and other professional where we need this to look after you (LI, PI).

5 We need to tell the appropriate teachers if you have a health issue (LI, PI).

6 We will need to tell your teachers if you have special educational needs or need extra help with some tasks (LI, PI).

7 We will need to share information about you (e.g. about your health and wellbeing) with the School's pastoral team (LI, PI, VI).

8 If we have information that you suffer from an allergy we will use this information so that we can look after you (LI, PI, VI).

9 If we have information that you suffer from a disability we will use information about that disability to provide support (LI, PI).

10 Where appropriate, the School will have information about your religious or other beliefs and practices. For example, if you do not eat certain foods (LI, PI).

11 We will also hold information such as your religion or ethnic group for the purposes of ensuring that any special needs are met (LI).

12 We use CCTV to make sure the School site is safe. Images captured of you via CCTV will be your personal data. CCTV is not used in private areas such as changing rooms (LI, PI).

13 We will use your personal data to take other steps to make sure the School site and buildings are safe, for example, at any given time] (LI, PI).

14 We record your attendance and if you have time away from the School we record the reason(s) why (LI, PI).

15 We will need to share some information about you with the government (e.g. the Department for Education). We will need to tell the local authority that you attend the School, if you leave the School or let them know if we have any concerns about your welfare. The local authority may also share information with us for these reasons (LI, LO, PI).

16 We may need to share information about you with the Health and Safety Executive (a government organisation) if there is a health and safety issue at the School (LI, LO).

17 The School is sometimes inspected to make sure that we are continuing to be a good School. We will have to make your information available to the inspectors to help them to carry out their job (LI, PI, LO).

18 We will need information about any court orders or criminal matters that relate to you. This is so that we can safeguard your welfare and wellbeing and the other pupils at the School (LI, PI).

19 If you are from another country we have to make sure that you have the right to study in the UK. Sometimes the government will ask us to provide information as part of our reporting requirements. In addition to this we have a duty to provide information about you to UK Visas and Immigration who are part of the government (LI, LO, PI).

20 Depending on where you will go when you leave us we will provide your information to other schools, Schools and universities, UCAS or potential employers. For example, we will share information about your exam results and provide references (LI, PI). If we hold safeguarding information about you, we will share that with your next School.

21 We may pass on information to your next school or School which they need to look after you, for example, information about any concerns we have had about your welfare (LI, LO, PI).

22 When you take public examinations (e.g. GCSEs or A-Levels) we will need to share information about you with examination boards. For example, if you require extra time in your exams (LI, PI,).

23 If someone makes a complaint about how the School has behaved we may need to use your information to deal with this appropriately. For example, if your parents complain that we have not looked after you properly (LI, PI).

24 The School may share information about you with the local authority for the purpose of the preparation, implementation and / or review of your Statement of Special Educational Needs or Education Health and Care Plan (LI, PI, LO).

25 We may use your information in connection with legal disputes (LI, PI, LO).

26 We may need to share information about you with the police or our legal advisers if something goes wrong or to help with an enquiry. For example, if one of your classmates is injured at School or if there is a burglary (LI, LO, PI).

27 We use consultants, experts and other advisors to assist the School in fulfilling its obligations and to help run the School properly. We will share your information with them if this is relevant to their work (LI, PI).

28 If you have misbehaved in a serious way, we may need to share information with the police and we may need to use information about the action taken by the police (LI, LO, PI).

29 We may share some information with our insurance company to make sure that we have the insurance cover that we need or in connection with an actual or possible claim (LI, PI).

30 If the School is dealing with a request for information, query, or complaint, we may sometimes need to share your information with the other people involved such as other pupils and their parents (LI, PI).

31 Parents who are based outside of the UK will sometimes choose someone to act on their behalf during the admissions process (an overseas consultant). If this applies to you, your parents may provide information to the overseas agent so that he or she can pass this on to the School. The School will sometimes share information with the overseas consultant, for example, we may send them the letter telling your parents that we are offering you a place so that they can pass this on to your parents (LI).

32 We will share your academic and (where fair) your behaviour records with your parents or education guardian so they can support your education (LI, PI).

33 If ever in the future, we are considering restructuring or selling our business we may share your information with the other parties involved and with the relevant professional advisors (LI).

34 We will monitor your use of email, the internet and mobile electronic devices e.g. iPads. In certain circumstances we will look at the content of your messages (e.g. emails and text messages). We monitor and look at your use of technology (e.g. your use of your phone) to check that you and your classmates are not misbehaving, at risk of harm or for other good reasons. If you would like more information about this you can read the acceptable use of IT and email policy or speak to a member of the admin team (LI, PI,). The monitoring we do is carried out using computer software which will automatically tell us if something isn't right.

35 We may use photographs or videos of you for the School's website and social media sites or prospectus to show prospective pupils what we do here and to advertise the School. We may continue to use these photographs and videos after you have left the School (LI, PI).

Sometimes we use photographs and videos for teaching purposes, for example, to record a drama lesson (LI, PI).

If you have concerns about us using photographs or videos of you please let us know.

36 We may use your personal data in order to help make the School better, for example, to raise money for the School, this includes sending you information about how you can donate to the School after you have left (LI). .

37 We may also use your personal data in order to promote education and learning more generally, for example, if we included a photograph of your class in an advert to encourage adults to take evening classes (PI) (LI).

38 We publish our public exam results, sports fixtures and other news on the website and put articles and photographs in the local news to tell people about what we have been doing (LI).

39 We will keep details of your address when you leave so we can keep you updated about what is happening at the School, to tell you about events and activities and find out how you are getting on. We may also pass your details onto the alumni organisation (LI).

40 The School must make sure that our computer systems are working well and are secure. This may involve information about you, for example, our anti-virus software might scan files containing information about you (LI).

41 We may share your information with the other Schools in the Group. For example, how well you have behaved and your test results (LI, PI).

42 Sometimes we use someone from outside of the School to provide activities. For example, this could be a teacher who does not normally work for the School or it could be a company that provides outdoor activities. We may share your information with them, for example, to tell them what sports you are good at (LI, PI).

43 Some of the records the School keeps and which contain your personal data may be used by the School (or by someone else such as the government) to check that the School has been a good School (LI, PI).

44 We also keep some information forever for archiving purposes and for historical research purposes. This includes the School's legitimate interest in keeping a record of what the School was like in the past. For example, we keep some old photographs so that we have a record of what the School was like in the past as this helps get people interested in the School's history. Information held in our archive may be made publicly available but this would only be done in compliance with data protection laws. Please speak to the admin team if you would like more information (LI, PI).

45 We will share your information with Governors of the School if it concerns something they should know about or which will enable them to fulfil their role as a School Governor. For example, this will apply if you have done something really well or if there is a problem at the School they need to know about (LI, PI).

We will only share your information with other people and organisations when we have a good reason to do so. In exceptional circumstances we may need to share it more widely than we would normally.

As you will see from the information above, in some cases we will rely on more than one lawful basis for using your information. In addition, we may move from one of the lawful bases listed above to another as circumstances change. For example, if we become really worried about your wellbeing, we may start to rely on "legal obligation" to share personal data with the local authority in addition to the other lawful bases that are noted for looking after you.

We may use third parties to handle personal data on our behalf for the following purposes:

a) IT consultants who help run the School's computer systems. For example, they might need to access a file containing personal data when investigating a fault or checking the security of our IT network;

b) We use software, apps and websites to help us with teaching, and to help us provide pastoral support to you and your classmates; and

c) We use third party "cloud computing" services to store some information rather than the information being stored on hard drives located on the School site.

If you have any questions about any of the above, please speak to us.

The School has extra obligations in relation to some types of more sensitive personal data. This applies to information about racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic information, biometric information, health information, information about sex life or orientation, information about criminal convictions or offences. When the School handles these types of information it will usually be doing so because:

- It is in the substantial public interest to do so, for example, to provide you with an education, to look after you and your classmates or when the School is inspected.
- For medical purposes. This includes medical treatment and the management of healthcare services.
- The School is an employer (e.g. we employ your teachers). Also the School will use your information to comply with social protection law (e.g. to look after you) and social security laws. Social protection law is concerned with preventing, managing, and overcoming situations that adversely affect people's wellbeing.
- To protect the vital interests of any person where that person cannot give consent, for example, if they are seriously hurt and are unconscious.
- It is necessary for the establishment, exercise or defence of legal claims. For example, this allows us to share information with our legal advisors and insurers.

Consent

We may ask for your consent to use your information in certain ways as an alternative to relying on any of the bases above. For example, we may ask for your consent before taking or using some photographs and videos if the photograph or video is more intrusive and we cannot rely on legitimate interests. If we ask for your consent to use your personal data you can take back this consent at any time.