



Hope Tree School
Where difference is valued

Data Protection and Freedom of Information Policy 2024

The UK General Data Protection Regulation (UK GDPR)

Introduction

Hope Tree School collects and uses certain types of personal information about staff, students, parents and other individuals who come into contact with the School in order to provide education and associated functions. The School may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the UK General Data Protection Regulation and other related legislation.

The UK GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

This policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every two (2) years.

This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. It reflects the ICO's code of practice for the use of surveillance cameras and personal information.

This policy complies with Regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the rights of access to their child's educational record

Definition Table

Term	Definition
Personal Data	<p>'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. This may include:</p> <p>Name (including initials) Identification Number Location Data (Address) Online Identifier (Username)</p> <p>It may also include factors specific to an individual's physiological, genetic, mental, economic, cultural or social identity.</p>
Special Category (Sensitive Data)	<p>A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:</p> <ul style="list-style-type: none"> ● race or ethnic origin; ● political opinions; ● religious or philosophical beliefs; trade union membership; ● physical or mental health; ● an individual's sex life or sexual orientation; ● genetic or biometric data for the purpose of uniquely identifying a natural person. <p>Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.</p>
Data Subject	The identifiable individual whose personal data is processed or held.
Data controller	The organisation that determines the purpose and the means of processing of personal data.

Data processor	A person or organisation who processes personal data on behalf of the data controller (not including the data controller or an employee).
Processing	Anything done to personal data, such as collecting, organising, storing, altering, using, erasing or destroying. Processing data can be a manual or automated process.
Data Protection Officer (DPO)	The Data Protection Officer is responsible for auditing the protection of data in the School, liaising with the ICO and responding to requests

The Data Controller

Hope Tree School processes personal data relating to parents, students, staff, governors, visitors and others and therefore is the data controller. The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

This policy applies to all staff employed by Hope Tree School. Staff who do not comply with this policy may face disciplinary action. The Proprietors have overall responsibility for ensuring that Hope Tree School complies with all relevant data protection obligations. The Head of Learning and Head of Pastoral Care act as representatives of the data controller on a day to day basis.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with the data protection law, and developing related policies and guidelines where applicable.

The DPO is the first point of contact for individuals and organisations whose data Hope Tree School processes, and for the ICO.

The DPO will provide a report to the School's Advisory Board for each meeting where relevant, reporting their advice, recommendations and any breaches. The DPO is Fiona D'Arcy and is contactable via admin@hopetreeSchool.co.uk

Staff are responsible for:

- Collecting, storage, processing, publishing any personal data in accordance with this policy.
- Informing the DPO of any changes to their living arrangements, personal data (i.e: new address, phone number, home email, living status etc)

- Contacting the DPO if they have any queries or questions regarding the use of and the protection of data within the School, including;
 - Concerns that the policy is not being followed
 - If they are unsure how to process a piece of personal data, including how they can store and transmit/receive data from external sources
 - If there has been a data breach
 - If they are unsure whether there is a lawful basis to collect and/or store information
 - Whenever they are engaging in a new activity that may affect the privacy rights of an individual, including the use of a new data processor and the upload of data to 3rd party companies such as new learning platforms where students need to login
 - If they need to apply a UK GDPR principle to processing data

The data protection principles

The UK GDPR is based on data protection principles that Hope Tree School must comply with:

1. Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
2. Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
3. Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
4. Personal data shall be accurate and, where necessary, kept up to date;
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
6. Personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

In addition, Hope Tree School is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law.

Hope Tree School is committed to complying with the principles at all times. This means the School will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
- ensure that when information is authorised for disposal it is done

appropriately;

- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests;
- report any breaches of the UK GDPR in accordance with the procedure outlined in this policy.

Collecting personal data:

Lawfulness, fairness and transparency

- We will only process personal data where we have one of the 6 'lawful bases' (legal reasons) to do so under the data protection law:
 - o The data needs to be processed so that the School can fulfil a contract with the individual, or the individual has asked the School to take specific steps before entering into a contract.
 - o The data needs to be processed so that the School can comply with a legal obligation.
 - o The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
 - o The data needs to be processed so that the School, as a public authority, can perform a task in the public interest, and carry out its official functions.
 - o The data needs to be processed for the legitimate interests of the School or a third party (provided the individual's rights and freedoms are not overridden).
 - o The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.
- For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.
- If we offer online services to students, e.g. educational/classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent when a student is under 13 (except for online counselling and preventive services).
- Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, minimisation and accuracy

- We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their job.
- When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Schools data retention policy.

Use of personal data by Hope Tree School

Hope Tree School holds personal data on students, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in this policy.

Students:

- The personal data held regarding students includes contact details, assessment results (including exams where appropriate), attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.
- The data is used in order to support the education of the students, to monitor and report on their progress and to provide appropriate pastoral care, in addition to any other uses normally associated with provision in a School environment.
- The School may make use of limited personal data (such as contact details) relating to students, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with families of students attending the School.

In particular, the School may:

- make personal data, including sensitive personal data, available to staff for planning curricular or extracurricular activities;
- use photographs of students in accordance with the guidance outlined in this policy.

Any individual wishing to limit or object to appropriate use of personal data should notify the DPO in writing. If, in the view of the DPO the objection cannot be maintained, the individual will be given written reasons why the School cannot comply with their request.

Staff:

- The personal data held about staff will include contact details, employment history, information relating to career progression, performance, information relating to DBS checks and photographs.
- The data is used to comply with legal obligations placed on the School in relation to employment, and the education of children in a School environment. The School may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.
- Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as “spent” once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.
- Any individual wishing to limit or object to the appropriate use of personal data should notify the DPO who will ensure that this is recorded, and adhered to if appropriate. If the DPO is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the School cannot comply with their request.

Other Individuals

- The School may hold personal information in relation to other individuals who have contact with the School, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

Security of personal data

Hope Tree School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the UK GDPR. The School will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

For further details as regards security of IT systems, please refer to the School’s Acceptable Use Policy.

Disclosure of personal data to third parties

The following list includes the most usual reasons that the School will authorise disclosure of personal data to a third party:

- Where this is outlined in our privacy notices
- Where there is an issue with a student or parent/carer that puts the safety of staff or students at risk
- To give a confidential reference relating to a current or former employee,

volunteer or student

- for the prevention or detection of crime
- for the assessment of any tax or duty
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings)
- for the purpose of obtaining legal advice
- for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress)
- to publish the achievements of the students attending the School
- to disclose details of a student's medical condition where it is in the students interests to do so, for example: -
 - for medical advice, insurance purposes or to organisers of School trips;
 - to provide information to another educational establishment to which a student is transferring;
 - to provide information to an Examination Authority as part of the examination process.
- Hope Tree School may also share personal data with emergency services and local authorities to help them respond in an emergency that affects any student, staff members or volunteers.
- The School may receive requests from third parties to disclose personal data it holds about a student, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned.

All requests for the disclosure of personal data must be sent to the Data Protection Officer (DPO) who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

Confidentiality of student concerns

Where a student seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the School will maintain confidentiality unless it has reasonable grounds to believe that the student does not fully understand the consequences of withholding their consent, or where the School believes disclosure will be in the best interests of the student or other students.

The safety of any student within the School or the School's care is paramount. Hope Tree School's Child Protection policy will always override any confidentiality concerns.

Subject Access Requests

Anybody who makes a request to see any personal information held about them by the School is making a subject access request (SAR). All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

All requests should be sent to the Data Protection Officer (DPO) in writing and must be dealt with in full without delay within 1 month of receipt of the request. Where a request is complex or numerous, the School may seek an extension. The School will inform the applicant of this within 1 month, explaining why the extension is necessary.

Subject access requests must be submitted in writing, either by letter or email, addressed to the Data Protection Officer. A template is available on the School website which includes:

Name of the individual

Correspondence address

Contact Number and email address

Details of the information requested

If a staff member receives a subject access request they must immediately forward the request to the Data Protection Officer.

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The DPO must, however, be satisfied that:

- the child or young person lacks sufficient understanding; and
- the request made on behalf of the child or young person is in their interests.

Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the School must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s). The School will provide the information free of charge, unless it is an unfounded or

excessive request. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

The requester may be asked to provide two forms of identification to prove who they are and to allow the School to ensure they are eligible to access the information and to ensure information is not released to the wrong parties.

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document or file cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

Exemptions to access by data subjects

Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.

The School will not disclose information if it:

- Might cause serious harm to the physical or mental health of the individual or another individual;
- Would reveal that a student is at risk of abuse or where the disclosure of that information would not be in the child's best interests;
- Is detailed in the court orders;
- Is information where disclosure would result in revealing personal information about another student, staff member, volunteer or visitor.

Other rights of individuals

The School has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the School will comply with the rights to:

- Object to Processing
- Rectification
- Erasure
- Portability

Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest.

Where such an objection is made, it must be sent to the DPO and the DPO will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The DPO shall be responsible for notifying the individual of the outcome of their assessment within 30 working days of receipt of the objection.

Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the DPO should be notified. The request and reasons for refusal shall be noted alongside the data, and communicated to the individual by the Data Protection Officer (DPO). The individual shall be given the option of a review under the complaints procedure, or an appeal directly to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- where consent is withdrawn and there is no other legal basis for the processing;
- where an objection has been raised under the right to object, and found to be legitimate;
- where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);
- where there is a legal obligation on the School to delete.

The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

- where the accuracy of data has been contested, during the period when the School is attempting to verify the accuracy of the data;
- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim.

Right to portability

If an individual wants to send their personal data to another organisation they have a right to request that the School provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the School is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the DPO and the DPO will review and revert as necessary.

Breach of the UK GDPR legislation

Any and all breaches of the UK GDPR, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Officer (DPO).

Once notified, the DPO shall assess:

- the extent of the breach

- the risks to the data subjects as a consequence of the breach
- any security measures in place that will protect the information
- any measures that can be taken immediately to mitigate the risk to the individuals

Unless the DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the School, unless a delay can be justified.

The Information Commissioner will be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries (which shall usually be the DPO);
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the DPO shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

The DPO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the proprietors and Advisory Board and a decision made about implementation of those recommendations.

Data security and Storage

The School will protect data from unauthorised or unlawful access, processing or disclosure and against accidental or unlawful loss, destruction, communication or damage.

The School will ensure that:

- Paper records and portable electronic devices (such as laptops and storage devices) that contain personal data are kept locked away when not in use.
- Documents containing confidential personal data will not be left on display in offices/classrooms, in staffrooms, pinned to display boards or left anywhere

where there is general public access.

- Personal data, where displayed in classrooms will conform to protection guidelines regarding sensitive information and the approval of its use.
- Where personal data is displayed in a room where members of the public are invited, information will be hidden out of view or covered when not in use.
- IT system passwords will be strong and changed regularly.
- Encryption software is used to protect all laptops.
- Staff, students, members of the advisory board and volunteers who store or process personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment.
- Where data is shared with a third party, the School will carry out due diligence and take reasonable steps to ensure it is stored and transmitted securely.
- Where a member of staff no longer works for the School, they will be asked to permanently delete any personal data they may hold on staff, students or parents and return any IT hardware or software provided by the School. To be clear this includes but is not limited to: books, registers, student reports, assessment/attainment data, child protection/ safeguarding records and photos of students.

Disposal of data

Personal data that is no longer needed will be disposed of securely. Data that has become inaccurate or out of date will be updated if there is a legal basis to maintain it, or deleted if no longer needed.

The disposal of data will be undertaken in accordance with the School's data retention policy.

Data marked for disposal will be securely destroyed, by shredding for paper-based records.

Training

All staff and volunteers are provided with data protection training as part of their induction.

Data protection training is also part of the CPD process for staff each year.

Where significant changes are applied to legislation, the School will make the necessary training available to ensure all staff are updated.

CCTV

The School uses CCTV in three locations to ensure the staff, students, site and resources remain safe and secure.

The School does not need to ask individuals' permission to use CCTV, however, it should ensure clear signage informing users that the site has CCTV and how to ask for more information.

Further information is available within the School's CCTV policy.

Photographs and Videos

As part of School activities, photographs and images of individuals who attend the School may be recorded.

Written consent will be obtained from parents/carers, or students, for photographs and videos to be taken of them/their child for communication, marketing and promotional materials across the School.

Where parental consent is needed, it will be clearly explained how the photograph and/or video will be used to the parent/carer or student. Where parental consent is not needed, it will be clearly explained to the student how the photograph and/or video will be used.

Uses may include:

- School Website
- School Prospectus
- School newsletters
- School noticeboard/celebration boards
- Outside of School by external agencies such as School photographer
- School social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the School will delete the photograph or video and not distribute further.

When using photographs and videos, personal data will not accompany them or any other personal information about the child, to reduce the risk of them being identified.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

Contact

If anyone has any concerns or questions in relation to this policy, they should contact the Data Protection Officer.

If at any time you are not happy with how the School is processing your personal information then you may raise the issue with the Data Protection Officer and if you are not happy with the outcome you may raise a complaint with the Information Commissioner's Office:
Information Commissioner's Office Wycliffe House

Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Freedom of Information

The Freedom of Information Act

The School is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

The Freedom of Information Act gives you the right to ask for all the recorded information the School has on any subject. Anyone can make a request for information – there are no restrictions on your age, nationality or where you live. Your request will be handled under the Data Protection Act 2018 if you ask for information about yourself.

Any request for any information from the School is technically a request under the FOI, whether or not the individual making the request mentions the FOI. However, the ICO has stated that routine requests for information (such as a parent requesting a copy of a policy) can be dealt with outside of the provisions of the Act.

In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the DPO.

All other requests should be referred in the first instance to the DPO.

Time limit for Compliance

The School must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. For a School, a “working day” is one in which students are in attendance, subject to an absolute maximum of 60 calendar days to respond.

Term dates can be found on the School website.

Procedure for responding to a FOI request

When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the School DPO.

The first stage in responding is to determine whether or not the School “holds” the information requested. The School will hold the information if it exists in computer or paper format.

The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

- Section 41 – information that has been sent to the School (but not the School’s own information) which is confidential
- Section 21 – information that is already publicly available, even if payment of a fee is required to access that information
- Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information)
- Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras.

How to make an FOI request

Contact us directly via email: admin@hopetreeSchool.co.uk to make a freedom of information (FOI) request.

When making your request, you should include:

- your name
- an address where you can be contacted (including e-mail)
- a detailed description of the recorded information you want

How you can receive the information

You can ask for the information in a number of different formats:

- paper or electronic copies of any documents
- audio format
- large print

Make sure you check the copyright status of the information you receive if you plan to reproduce it. It is your responsibility to check this. The School or any representative shall not be held liable for your failure to check this.

If your request is turned down, what can you do about it?

Some sensitive information might not be available to members of the public. If this is the case, we will tell you why we have withheld some or all of the information you requested.

The School can turn down your request if we think it will cost more than £450 to deal with your request.

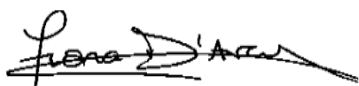
The School might ask you to be more specific so we can provide the information you’re looking for.

If the School doesn't provide you with the information you request, you should first contact them asking to review the decision. If you are still not satisfied, you can complain to the Information Commissioner's Office. – www.ico.org.uk

Signed:

A handwritten signature in blue ink, appearing to read 'P. Sande'.

Head of Learning

A handwritten signature in black ink, appearing to read 'Liona D'Arcy'.

Head of Pastoral Care

Date: March 2024

Review Date: March 2025