Data Protection Policy

The Olive Tree
Primary School

Document Control

This document has been approved for operation at The Olive Tree Primary School	
Date of approval:	24/06/2024
Date of next review:	June 2025
Review period:	As required / 12 months
Status:	Approved
Approval Committee:	FHBC
Version:	V2.0

Contents

Scope of Policy

The aim of this policy is to clarify how personal information is dealt with properly and securely and in accordance with the UK General Data Protection Regulation (GDPR) and other related legislation. It applies to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically. It applies to all data held by the Trust or The Olive Tree Primary School.

Introduction

The Olive Tree Primary School collects and uses certain types of personal information about staff, pupils, parents, trustees and other individuals who come into contact with the School in order to provide education and associated functions. The School may also 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 confirms how that personal information is dealt with properly and securely, and in accordance with GDPR and other legislation.

What is GDPR?

There are now two General Data Protection Regulations: in the European Economic Area (the EEA GDPR) and in the United Kingdom (as tailored by the Data Protection Act, the UK GDPR). Both the EEA GDPR and the UK GDPR regulate the collection, use, transfer, storing, and other processing of personal data of persons in their respective jurisdictions.

To which persons do the EEA GDPR and UK GDPR apply?

The EEA GDPR and the UK GDPR apply to all persons. There is no requirement that a person be a citizen or resident of a country that is a member of the EEA or of the UK.

To what countries does the EEA GDPR apply? What are the EU and the EEA?

The EEA GDPR applies to all member countries of the European Union (EU). It also applies to all countries in the European Economic Area (the EEA). The EEA is an area larger than the EU and includes Iceland, Norway, and Liechtenstein. As of January 1, 2021, the UK is no longer a member of the EU and is no longer subject to the EEA GDPR.

When do the EEA GDPR and the UK GDPR apply?

There are three types of situations that are subject to the EEA GDPR and UK GDPR:

1. If a person is present in the EEA or the UK, any personal data collected from them in connection with the offering of a good or service is protected by that area's GDPR, even if the organisation offering the good or service is not established in that area. Protection for the personal data continues after the person leaves the EEA or the UK.
2. Establishments in the EEA or UK. If personal data is collected or otherwise processed in the context of the activities of any establishment in the EEA or UK, then the personal data is protected by that area's GDPR, even if the processing occurs outside the EEA or the UK.
3. If a person is present in the EEA or UK, any personal data collected from them in connection with the monitoring of their behaviour where the behaviour takes place within the EEA or the UK.

To what data do the EEA GDPR and the UK GDPR apply?

The EEA GDPR and the UK GDPR apply to all "personal data," which includes any information relating to a living, identified or identifiable person. Examples include name, identification numbers, location data, IP addresses, online cookies, images, email addresses, and content generated by the data subject.

The EEA GDPR and the UK GDPR include more stringent protections for special categories of personal data. These are:

- Racial or ethnic origin
- Physical or mental health data
- Political opinions

- Sex life and sexual orientation
- Religious or philosophical beliefs
- Genetic and biometric data
- Trade union membership

The EEA GDPR and the UK GDPR also impose limitations on the processing of personal data relating to criminal convictions and offences.

Roles and Responsibilities

The Olive Tree Primary School is a registered data controller. The Board of Trustees is ultimately accountable for ensuring that the School complies with all relevant legislation including for data protection.

The School Business Manager (SBM) serves as the Schools' Data Protection Partner, responsible for overall coordination of data protection including Information Commissioner's Office (ICO) registration and overseeing responses to subject access requests, and data breach investigations with support from the Senior Leadership Team and the trust governance partner Hill Dickinson LLP.

All staff are made aware of this policy and their duties under GDPR as part of their induction to the School. In addition, regular training opportunities are made available to staff, in particular those for whom data protection is of particular relevance to their role.

Personal data

'Personal data' is any information that identifies an individual. It 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(1). A sub-set of personal data is known as 'special category personal data' (previously known as sensitive personal data).

(1) *For example, if you were asked for the number of male employees, and you only have one male employee, this would be classed as personal data if it was possible to obtain a list of employees from the school website*.

Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is a legal authority to do so.

The Olive Tree Primary School does not intend to seek or hold Special Category Data about staff or pupils except where we have been notified of the information, or it comes to the attention of the School via legitimate means (e.g., a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the School their race or ethnic origin, political or religious beliefs, whether they are a trade union member or details of their sexual life (save to the extent that details of marital status and/or parenthood are needed for other purposes, e.g., pension entitlements).

Data Protection Principles

The six data protection principles as laid down in the GDPR are always followed:

- 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.
- Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes.
- Personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for the original purpose(s).
- 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 to this, the School is committed to always ensuring that, anyone dealing with personal data shall be mindful of the individual's rights under the law.

The School is committed to complying with the data protection principles and as such will:

- Inform individuals about how and why we process their personal data through our pupil, staff and trustee privacy policies.
- Be responsible for checking the quality and accuracy of the information through our annual pupil and staff data collection exercise.
- 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 schedule.
- Ensure that when information is authorised for disposal it is done appropriately.
- Ensure appropriate security measures to safeguard personal information, whether held in paper files or electronically, and always follow the relevant security policy requirements.
- Only share personal information with others 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 (SAR).

Report any breaches of GDPR using the ICO '[Report a data breach online form]'.

Conditions for processing personal data in the first Data Protection principle

The individual has given consent that is specific to the processing activity, and that consent is informed, unambiguous and freely given.

The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

The processing is necessary for the performance of a legal obligation to which we are subject.

The processing is necessary to protect the vital interests of the individual or another.

The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

Outside of fulfilling our public task, the processing is necessary for a legitimate interest of The Olive Tree Primary School or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

Use of personal data by The Olive Tree Primary School

The School processes personal data on pupils, staff, trustees and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined above.

Pupils

The personal data held regarding pupils includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

The data is used to support the education of pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well The Olive Tree Primary School is doing, together with any other uses normally associated with this provision in a school environment. Personal data may also be used to maintain behaviour or safeguarding records.

The School may make use of limited personal data (such as contact details) relating to pupils, and their parents, carers or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, but only where consent has been provided for this.

In particular, the School may:

- transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the School but only where consent has been obtained first;
- make personal data, including sensitive personal data, available to staff for planning curricular or extracurricular activities.

- keep the pupil's previous setting informed of their academic progress and achievements e.g., sending a copy of the school reports for the pupil's first year at the School to their previous school.
- Use photographs of pupils in accordance with the E-Safety policy and associated photography procedures.

Use pupil personal data to ensure necessary access to online resources can be maintained to facilitate both classroom and remote learning.

Any wish to limit or object to any use of personal data should be notified to the school Data Protection Lead in writing, which will be acknowledged by the school in writing. If, in the view of the school Data Protection Lead and the Trust Data Protection Partner the objection cannot be maintained, the individual will be given written reasons why the School cannot comply with their request. This decision can be appealed in writing to the Chair of the Board of Trustees % clerk to the board of the trustees or the ICO.

Staff

The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks and photographs, as well as information required to administer the terms and conditions of employment including occupational pensions.

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 wish to limit or object to the uses of personal data should be notified to the school Data Protection Lead and the Trust Data Protection Partner who will ensure that this is recorded and adhered to if appropriate. If the school Data Protection Lead and Trust Data Protection Partner are 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. This decision can be appealed to the Chair of the Board of Trustees % the clerk to the board of trustees or the ICO.

Information relating to DBS checks

DBS checks are carried out based on the School's legal obligations in relation to Keeping Children Safe in Education (KCSIE) and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Data Retention Schedule.

Access to the DBS information is restricted to individuals who have a genuine need to have access to it for their job roles. In addition to the provisions of the GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

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

The 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 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 E-Safety Policy. The School' Incident Response Strategy outlines how data kept on the School's servers/cloud-based storage will be kept secure, and then recovered, in the event of a major incident.

Disclosure of personal data to third parties

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

- To give a confidential reference relating to a current or former employee, volunteer or pupil.
- For the prevention or detection of crime.
- For the assessment of any tax or duty.
- For administration of pensions and employee benefits.
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the School (other than an obligation imposed by contract).
- 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 results of public examinations or other achievements of pupils of the School.
- To disclose details of a pupil's medical condition where it is in the pupil's interests to do so and there is a legal basis for doing so, for example for medical advice, insurance purposes or to organisers of school trips. The legal basis will vary in each case but will usually be based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals).
- To provide information to another educational establishment to which a pupil is transferring.
- To provide information to the Examination Authority as part of the examination process.
- To provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal

data with other Government Departments or agencies strictly for statistical or research purposes.

The School may receive requests from third parties (i.e., those other than the data subject, The School, and employees of The School) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will generally be disclosed, including where the information is necessary for the legitimate interests of the individual concerned or The School, unless one of the specific exemptions under data protection legislation applies.

All requests for the disclosure of personal data must be sent to the School Data Protection Partner, 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 pupil concerns

Where a pupil 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 pupil does not fully understand the consequences of withholding their consent, or where The School believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest.

Subject access requests (SAR)

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

The individual's full subject access right is to know:

- Whether personal data about them is being processed.
- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom their personal data have been or will be disclosed.

- The envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored.
- The existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing.
- The right to lodge a complaint with the ICO.
- Where the personal data are not collected from the individual, any available information as to their source.
- Details of the safeguards in place for any transfers of their data to locations outside the European Economic Area.

All requests must be acknowledged within two School working days of receipt and must be dealt with in full without delay, at the latest within one month of receipt.

Where a child or young person does not have sufficient understanding to make their own request (usually those under the age of thirteen, or thirteen and over 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 Data Protection Partner must, however, be satisfied that:

- The child or young person lacks sufficient understanding.
- 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 Data Protection Partner 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).

A subject access request must be acknowledged in writing. The School may ask for any further information reasonably required to locate the information.

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 Data Protection Partner before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document 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 The School intends to apply any of them to a request then The School will usually explain which exemption is being applied and why.

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.
- Data 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 where they do not believe that those grounds are adequately established.

Where such an objection is made, it must be sent to the school Data Protection Lead and the School Data Protection Partner within two working days of receipt by the school, who 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 school Data Protection Lead and the School Data Protection Partner shall be responsible for notifying the individual of the outcome of their assessment within twenty working days of receipt of the objection.

Right to rectification – inaccurate personal data that should be corrected

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the school Data Protection Lead and The School Data Protection Partner within two working days of receipt by the school, 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 request and reasons for refusal shall be noted alongside the data and communicated to the individual. This decision can be appealed to the Chair of the Board of Trustees or the ICO.

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 – the right to be forgotten

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(s) 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 school Data Protection Lead and the School Data Protection Partner will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in 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 – where data processing needs to be paused

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.
- Where there has been an objection made under Article 21(1), and consideration is being given to whether the School legitimate grounds override those of the individual.

Right to portability – where data needs to be transferred

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 based on consent or performance of a contract, the situations in which this right can be exercised will be limited. If a request for this is made, it should be forwarded to the school Data Protection Lead and the School Data Protection Partner within two working days of receipt by the school, who will review and revert as necessary.

Breach of any requirement of the GDPR

All breaches of the GDPR or the confidentiality, integrity or availability of any personal data, including a breach of any of the data protection principles, shall be reported as

soon as it is/ they are discovered, to the school Data Protection Lead and The School Data Protection Partner.

Once notified, the The School Data Protection Partner shall assess:

- The extent of the breach.
- The risks to the data subjects because 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 School Data Protection Partner concludes that there is unlikely to be any risk to the rights or freedoms of individuals from the breach, it must be notified to the ICO within seventy-two hours of the breach having come to the attention of The School, unless a delay can be justified.

The ICO shall 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 School Data Protection Lead).
- 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 School Data Protection Partner or a member of the schools Senior Leadership Team 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 School Data Protection Lead under guidance from the School Data Protection Partner 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 made by the

Data Protection Partner and the school's Senior Leadership Team and a decision made about implementation of those recommendations.

Data Protection Complaints Procedure

The School aims to comply fully with its obligations under the GDPR. If you have any questions or concerns regarding The management of personal data by the school including your subject rights, please contact the School Data Protection Lead (admin@theolivetreeprimary.com).

If the School holds inaccurate information about you, contact the Data Protection Lead (admin@theolivetreeprimary.com) explaining what the problem is and where appropriate provide supporting documentation to show what the information should say. It is advisable to keep copies of the correspondence. If after a reasonable amount of time (twenty-eight days is recommended) the information has not been corrected, you can make a complaint.

If you feel that your questions/concerns have not been dealt with adequately on any data protection matter please get in touch with the school Data Protection Partner % The Olive Tree Primary School, Adelaide House, Adelaide Street, Bolton, BL3 3NY and the matter will be escalated to the Chair of the Board of Trustees.

If you remain unhappy with our response or if you need any advice you can contact the ICO. Please visit their website for information on how to make a data protection complaint.

The Freedom of Information Act gives any individual the opportunity to request information which we keep. Statutory Guidance on the Act can be found at www.ico.org.uk

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.

Freedom of Information (FOI) requests should be submitted by e-mail to: headteacher@theolivetreeprimary.com

Requests made in writing should be sent to: Freedom of Information, The Olive Tree Primary School, Adelaide House, Adelaide Street, Bolton BL3 3NY.

In order to be valid an FOI request must: be in writing (this includes electronic requests); be legible; include the requester's real name; include an address for correspondence; and describe the information being requested.

When considering a request under FOI, please bear in mind that a release under FOI is treated as a release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

Further information can be found in the school FOI & Publication Scheme.

Time limit for compliance with FOI requests

We will comply with timescales set by the Information Commissioner in responding to requests. If a request is particularly complex, we will assess how long it is likely to take to retrieve the relevant information. If it is more than 18 hours of staff time, we will levy a charge. In this case, we will write to advise the individual of the cost and they can decide whether to continue.

If the Trust receives two or more related requests within a period of 60 consecutive working days, from a person or different persons who appear to be acting in concert or in pursuance of a campaign, the costs of complying with the individual requests will be aggregated.

There are a range of exemptions that could apply, as allowed within the statutory guidance, for example if releasing information breaches commercial confidence or if there are other legal issues preventing disclosure.

Common exemptions include:

- Section 40 (1) – the request is for the applicant's personal data. This must be dealt with under the subject access regime in the GDPR, detailed in paragraph 10 above.
- Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the GDPR principles as set out in paragraph 4.1 of the policy above.
- Section 41 – information that has been sent to The School (but not The School' 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 22 – information that The School intends to publish at a future date.
- Section 43 – information that would prejudice the commercial interests of The School and/or a third party.

- 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.
- Section 36 – information which, in the opinion of the chair of trustees of The School, would prejudice the effective conduct of The School. There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

We will write to the individual if this applies.

When responding to a request where the School has withheld some or all the information, The School must explain why the information has been withheld, quoting the appropriate section number and explain how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

Individuals requesting information have the right to appeal the decision in writing to The Olive Tree Primary School in the first instance and to the Information Commissioner's office if they think the decision is unreasonable.

Please refer to the Trust FOI & Publication Scheme for detail on classes of information that are available, including our charging policy.

Freedom of Information (FOI) requests should be submitted by e-mail to: headteacher@theolivetreeprimary.com

Requests made in writing should be sent to: Freedom of Information, The Olive Tree Primary School, Adelaide House, Adelaide Street, Bolton BL3 3NY.

In order to be valid an FOI request must: be in writing (this includes electronic requests); be legible; include the requester's real name; include an address for correspondence; and describe the information being requested.

Concerns, questions or complaints in relation to this policy or the FOI Publication Scheme should be sent to the School Data Protection Partner % The Olive Tree Primary School, Adelaide House, Adelaide Street, Bolton. BL3 3 NY.

If you require a paper version of any information set out under the FOI Publication Scheme, or want to ask whether information is available, contact the School using the details set out above.

If you are not satisfied with the assistance that you get or if we have not been able to resolve your complaint and you feel that a formal complaint needs to be made then this should be addressed to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5A, telephone: 0303 123 1113, website: www.ico.org.uk