

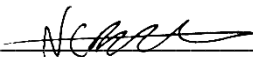


Prepared by:

Signature:

Date:


Neil Beattie
Compliance Manager



16th September 2024

Approved by:

Tony Lacey
Chief Executive Officer



16th September 2024

Jane Owens
Chair of Trustees



16th September 2024

Contents

1. Introduction	Page 3
2. Aims and objectives.....	Page 3
3. Data protection principles	Page 3
4. Data Protection Officer	Page 4
5. Data types	Page 4
6. Definitions	Page 5
7. Responsibilities	Page 6
8. Risk management roles	Page 7
9. Legal requirements and lawful processing	Page 8
10.Information for data subjects	Page 8
11. Consent	Page 8
12. The right of access	Page 8
13. The right to rectification	Page 9
14. The right to erasure	Page 9
15. The right to restrict processing	Page 10
16. The right to data portability	Page 10
17. The right to object	Page 11
18. Transporting, storing and deleting personal data	Page 11
19. Systems to protect data	Page 13
20. Data Breach – Procedure	Page 13
21. Summary of data security measures and procedures	Page 14
22. Subject Access Requests – Procedure	Page 15
23. Policy Review	Page 21

1. Introduction

Oak Trees Multi Academy Trust and our schools handle increasing amounts of personal information and have a statutory requirement to comply with The UK Data Protection Act and GDPR 2018. Oak Trees MAT and our schools have clear policies and procedures for dealing with personal information and are registered with the Information Commissioner's Office (ICO). Systems are in place to reduce the chances of a loss of personal information, otherwise known as a data breach, which could occur as a result of, for example, theft, loss, accidental disclosure, equipment failure or hacking.

Oak Trees Multi Academy Trust will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

2. Aims & Objectives:

The aim of this policy is to provide a framework to understand:

- The law regarding Personal and Special Category Data
- How Personal and Special Category data should be processed, stored, archived, and deleted/destroyed
- How you can access your records

Oak Trees Multi Academy Trust is required to keep and process certain information about everyone within its community in accordance with its legal obligations under the UK Data Protection Act and GDPR 2018. We may, from time to time, be required to share Personal and Special Category Data about its staff or pupils with other organisations, other schools and educational bodies, and, potentially, children's services. This policy is in place to ensure all staff and Governors are aware of their responsibilities and outlines how the school complies with the following core principles of The UK Data Protection Act and GDPR 2018.

This policy has due regard to legislation, including, but not limited to the following:

- The UK
- Data Protection Act and GDPR 2018
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

3. Data Protection Principles

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data
- Accountability, integrity and confidentiality

The Data Protection Act and GDPR 2018 also requires that the Data Controller shall be responsible for, and able to demonstrate, compliance with the principles.

4. Data Protection Officer (DPO)

A DPO has been appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the Data Protection laws
- Monitor the school's compliance, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members
- The individual or company appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools
- The DPO will report to the Compliance Manager
- The DPO will operate independently and will not be dismissed or penalised for performing their task
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations

5. Data Types

Not all data needs to be protected to the same standards, the more sensitive or potentially damaging the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. The UK DPA and GDPR UK defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal and/or Special Category Data is a Potential Data Breach, which could result in legal action against the school. The loss of Special Category Data is considered much more seriously and the sanctions may well be more punitive.

5.1. Personal Data

- The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:
- Personal information about members of the school community – including pupils, members of staff, parents / carers, volunteers, governors and trustee's names, addresses, contact details, DOB etc
- Curricular / academic data including class lists, pupil progress records, reports, references
- Professional records including employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

5.2. Special Category Data

Sensitive personal data is defined as information that relates to the following categories:

- Race and ethnicity
- Political opinions
- Religious or philosophical beliefs
- Membership of trade unions
- Physical or mental health
- Genetic data
- Biometric data
- Sex life
- Sexual orientation

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply.

On some occasions it is important that medical information should be shared more widely to protect a child - for instance if a child had a nut allergy how it should be treated. Where appropriate written permission should be sought from the parents / carers before posting information more widely.

5.3. Other types of Data not covered

This is data that does not identify a living individual and therefore is not covered by the remit of the Data Protection Act and GDPR 2018 but may fall under other access to information procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources, and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school.

6. Definitions

6.1. Personal data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

6.2. Special Category Data and Data Relating to Criminal Convictions and Offences

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data.

Personal data relating to criminal offences and convictions is included here for the purposes of this policy.

6.3. Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

6.4. Data Controller

The organisation storing and controlling such information (i.e., the School) is referred to as the Data Controller.

6.5. Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

6.6. Automated Processing

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

6.7. Data Protection Impact Assessment (DPIA)

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

6.8. Criminal Records Information

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

7. Responsibilities

The Headteacher in each school and the Board of Trustees are responsible for Data Protection.

8. Risk Management - Roles

The schools Data Protection Assessor is the Head Teacher and Their responsibilities are:

- Determine and take responsibility for the school's information risk policy and risk assessment
- Appoint the Information Asset Owners (IAOs)

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the school. Their role is to understand what information is held, what is added and what is removed,

how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.

The school will identify Information Asset Owners (IAOs).

The IAOs will manage and address risks to the information and will understand:

- What information is held, for how long and for what purpose
- How information has been amended or added to over time
- Who has access to protected data and why

8.1. Risk management - Staff and Governors and Board of Trustees Responsibilities

- Everyone in the school and Oak Trees MAT has the responsibility of handling personal information in a safe and secure manner
- Everyone in the school is expected to follow all processes and procedures in handling data
- Governors and the support staff at Head Office are required to comply fully with this policy in the event that they have access to personal data, when engaged in their roles

9. Legal Requirements and lawful processing

9.1. Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. The legal basis for processing data will be identified and documented prior to data being processed.

9.2. Lawful processing

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained
- Processing is necessary for:
 - Compliance with a legal obligation
 - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
 - For the performance of a contract with the data subject or to take steps to enter into a contract
 - Protecting the vital interests of a data subject or another person
 - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks)

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

10. Information for Data Subjects

To comply with the fair processing requirements, the school will inform the school community of the data they collect and process, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The Data Privacy Notice is available on each school's website and Oak Trees MAT website.

11. Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes
- Where consent is given, a record will be kept documenting how and when consent was given
- The school ensures that consent mechanisms are compliant. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease
- Consent can be withdrawn by the individual at any time

12. The right of access

- Individuals have the right to obtain confirmation that their data is being processed
- Individuals have the right to submit a subject access request (SAR) to gain access to their personal data to verify the lawfulness of the processing
- The school will verify the identity of the person making the request before any information is supplied
- SARs requested for pupils over the age of 13 will be subject to consent to share the data being obtained from the pupil before the request is processed
- A copy of the information will be supplied to the individual free of charge; however, the school may impose a reasonable fee to comply with requests for further copies of the same information
- Unless otherwise requested, the information requested will be provided in digital format
- Where a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information
- All requests will be responded to without delay and at the latest, within one month of receipt

- In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal
- If a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to

13. The right to rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified
- Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible
- Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to
- Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex
- Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority

14. The right to erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- Individuals have the right to erasure in the following circumstances:
 - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
 - When the individual withdraws their consent
 - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
 - The personal data was unlawfully processed
 - The personal data is required to be erased in order to comply with a legal obligation
- The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
 - To exercise the right of freedom of expression and information
 - To comply with a legal obligation for the performance of a public interest task or exercise of official authorities
 - For public health purposes in the public interest
 - For archiving purposes in the public interest, scientific research, historical research or statistical purposes
 - The exercise or defence of legal claims
- As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time

of the request. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so

- Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question

15. The right to restrict processing

- Individuals have the right to block or suppress the school's processing of personal data
- If processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future
- The school will restrict the processing of personal data in the following circumstances:
 - Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
 - Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
 - Where processing is unlawful and the individual opposes erasure and requests restriction instead
 - Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
 - If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so
 - The school will inform individuals when a restriction on processing has been lifted

16. The right to data portability

- Individuals have the right to obtain and reuse their personal data for their own purposes across different service
- Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability
- The right to data portability only applies in the following cases:
 - To personal data that an individual has provided to a controller
 - Where the processing is based on the individual's consent or for the performance of a contract
 - When processing is carried out by automated means
- Personal data will be provided in a structured, commonly used and machine-readable form
- The school will provide the information free of charge
- Where feasible, data will be transmitted directly to another organisation at the request of the individual
- The school is not required to adopt or maintain processing systems which are technically compatible with other organisations
- If the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual
- The school will respond to any requests for portability within one month

- Where the request is complex, or several requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request
- Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy

17. The right to object

- The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information
- Individuals have the right to object to the following:
 - Processing based on legitimate interests or the performance of a task in the public interest
 - Direct marketing
 - Processing for purposes of scientific or historical research and statistics
- Where personal data is processed for the performance of a legal task or legitimate interests
- An individual's grounds for objecting must relate to his or her particular situation
 - The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- Where personal data is processed for direct marketing purposes
 - The school will stop processing personal data for direct marketing purposes as soon as an objection is received
 - The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes
- Where personal data is processed for research purposes
 - The individual must have grounds relating to their particular situation in order to exercise their right to object
 - Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data
- Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online

18. Transporting, Storing and Deleting Personal Data

The policy and processes of the school will comply with the guidance issued by The Information Commissioner Office.

18.1. Information security - Storage and Access to Data

18.1.1. Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e.owned by the users) must not be used for the storage of personal data
- The school has a clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups

18.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

18.3. Passwords

All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable not to record complete passwords, but prompts could be recorded.

18.4. Images

- Images of pupils will only be processed and transported by use of encrypted devices
- Images will be protected and stored in a secure area

18.5. Cloud Based Storage

The school has clear policy and procedures for the use of Cloud Based Storage Systems and is aware that data held in remote and cloud storage is still required to be protected in line with the UK Data Protection Act and GDPR. The school will ensure that it is satisfied with controls put in place by remote / cloud-based data services providers to protect the data

18.6. Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a third party. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party and, where required, a Data Protection Impact Assessment will be completed before data is transferred.

18.7. Retention of Data

- Government guidance will be used to determine how long data is retained

- Personal data that is no longer required will be destroyed and this process will be recorded

19. Systems to protect Data

19.1. Paper Based Systems

- All paper based official or official sensitive (or higher) material must be held in lockable storage, whether on or off site
- Paper based personal information sent to parents will be checked by a member of the senior management team before the envelope is sealed

19.2. School Websites

Uploads to the school website will be checked prior to publication ensure that personal data will not be accidentally disclosed and that images uploaded only show pupils where prior permission has been obtained

19.3. E-mail

E-mails containing sensitive information should be encrypted, for example by attaching the sensitive information as a password protected word document. The recipient will then need to contact the school for access to a one-off password

20. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information

- In the event of a data breach the DPO will inform Oak Trees MAT and the head teacher
- The term personal data breach refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
- The headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their annual Data Protection training
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed
- All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case by-case basis
- If a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly
- A high risk breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority
- If a breach is sufficiently serious, the public will be notified without undue delay
- Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified
- Within a breach notification, the following information will be outlined:
 - The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
 - The name and contact details of the DPO

- An explanation of the likely consequences of the personal data breach
 - A description of the proposed measures to be taken to deal with the personal data breach
 - Where appropriate, a description of the measures taken to mitigate any possible adverse effects
-
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself

21. A summary of Data Security measures and procedures

- Confidential paper records are kept compliantly and destroyed ASAP
- Confidential paper records are not to be left unattended or in clear view anywhere with general access
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet or storage wall, drawer or safe when not in use
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted
- All electronic devices are password-protected to protect the information on the device in case of theft
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft
- Staff and governors do not use their personal laptops or computers for school purposes unless they are personally password-protected and fully encrypted
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data
- Before sharing data, all staff members ensure:
 - They are allowed to remove it
 - That adequate security is in place to protect it
- Under no circumstances are visitors allowed access to confidential or personal information
- Visitors to areas of the school containing sensitive information are supervised at all time
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place
- Our school takes its duties seriously and any unauthorised disclosure may result in disciplinary action
- The school business manager/Office manager (SBM) is responsible for continuity and recovery measures are in place to ensure the security of protected data

- Pupils assessment information is held on Assessment Manager. This is password protected and encrypted and only accessible to relevant staff
- Pupil data is held within digital Management Information Systems. Multi Factor Authentication has been activated and access is only available to relevant staff
- The school utilises a strong system of firewalls to deter any internet attack
- All staff emails are password protected
- All devices that can access pupil, staff details are password protected

22. Subject Access Requests

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A data subject has the right to be informed by the School of the following: -

1. Confirmation that their data is being processed;
2. Access to their personal data;
3. A description of the information that is being processed;
4. The purpose for which the information is being processed;
5. The recipients/class of recipients to whom that information is or may be disclosed;
6. Details of the School's sources of information obtained;
7. In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
8. Other supplementary information.

22.1. How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- For confirmation as to whether the School process personal data about him or her and, if so
- For access to that personal data
- And/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

22.2. How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

22.3. What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the Business or Office manager and Head Teacher who should contact E2E as DPO in order to assist with the request and what is required. The Compliance Manager or Head Office should also be informed. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

22.4. Acknowledging the Request

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request. In addition to acknowledging the request, the School may ask for:

- Proof of ID (if needed);
- Further clarification about the requested information;
- If it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- Consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

22.5. Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

22.6. Requests Made by Third Parties or on Behalf of Children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- The child's level of maturity and their ability to make decisions like this;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;
- Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 13 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 13 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

22.7. Fee For Responding to a SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

22.8. Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

22.9. School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the School will be closed/no one will be on site to comply with the request during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

22.10. Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- The purpose for which we process the data;
- The recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- Where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The fact that the individual has the right:
- To request that the Company rectifies, erases or restricts the processing of his personal data; or
- To object to its processing;
- To lodge a complaint with the ICO;

- Where the personal data has not been collected from the individual, any information available regarding the source of the data;
- Any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

22.11. How to Locate Information

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused. Depending on the type of information requested, the School may need to search all or some of the following:

- Electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- Manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- Data systems held externally by our data processors;
- Occupational health records;
- Pensions data;
- Share scheme information;
- Insurance benefit information.

The School should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

22.12. Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- The other individual has consented to the disclosure; or

- It is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- The type of information that they would disclose;
- Any duty of confidentiality they owe to the other individual;
- Any steps taken to seek consent from the other individual;
- Whether the other individual is capable of giving consent; and
- Any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

22.13. Other Exemptions to the Right of Subject Access

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- Education, training or employment of the individual;
- Appointment of the individual to any office; or
- Provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

22.14. Refusing to Respond to a Request

The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the school can:

- Request a "reasonable fee" to deal with the request; or
- Refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

22.15.Record Keeping

A record of all subject access requests shall be kept by the School, DPO and Head Office. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

23. Policy Review

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate and will usually be reviewed and updated yearly. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Trust.