The Oak Trust

Data Protection Policy

Oak Trust
Inspirational Learning & Leadership

Contents

1 Policy statement

1.1 Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as The Oak Trust we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.

1.2 We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

1.3 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.4 All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

2 About this policy

2.1 The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the [Data Protection Act 2018], and other regulations (together '**Data Protection Legislation**').

2.2 This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in the Annex to this policy.

4 Data Protection Officer

4.1 As a Multi Academy Trust we are required to appoint a Data Protection Officer (DPO). Our DPO is Mrs Janet Eppleston and she can be contacted at dpo@theoaktrust.org.uk.

4.2 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

4.3 The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **processed** fairly and lawfully and transparently in relation to the **data subject**

5.1.2 **processed** for specified, lawful purposes and in a way which is not incompatible with those purposes

5.1.3 adequate, relevant and not excessive for the purpose

5.1.4 accurate and up to date

5.1.5 not kept for any longer than is necessary for the purpose

5.1.6 **processed** securely using appropriate technical and organisational measures.

5.2 **Personal data** must also:

5.2.1 be **processed** in line with **data subjects'** rights

5.2.2 not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by The Oak Trust.

6 Fair and lawful processing

6.1 Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**

6.2.2 why the **personal data** is being **processed**

6.2.3 what the lawful basis is for that **processing** (see below)

6.2.4 whether the **personal data** will be shared, and if so with whom

6.2.5 the period for which the **personal data** will be held

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

6.4 For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract

6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g the Education Act 2011)

6.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest

6.4.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5 When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence

6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment

6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities

6.5.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.

6.6 We will inform **data subjects** of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8 There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.9 Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils and or our **workforce** join The Oak Trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, among other things. Where appropriate third parties may also be required to complete a consent form.

6.12 In relation to all pupils under the age of 13 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who has reached the age of 13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

6.14 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

6.14.1 inform the **data subject** of exactly what we intend to do with their **personal data**

6.14.2 require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in

6.14.3 inform the **data subject** of how they can withdraw their consent.

6.15 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

6.16 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.17 A record must always be kept of any consent, including how it was obtained and when.

7 Processing for limited purposes

7.1 In the course of our activities as The Oak Trust, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.

8 Notifying data subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as d**ata controller** and those of the DPO

8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**

8.1.4 whether the **personal data** will be transferred outside the European Economic Area (**EEA**) and if so the safeguards in place

8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy

8.1.6 the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.

9 Adequate, relevant and non-excessive processing

9.1 We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

9.2 Staff must only process personal data where it is necessary in order to do their job. When staff no longer need the personal data they hold they must ensure it is deleted or anonymised. This will be done in accordance with the Trusts Retention and Destruction Policy.

10 Accurate data

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11 Timely processing

11.1 We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.

12 Processing in line with data subject's rights

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

12.1.1 request access to any **personal data** we hold about them

12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing

12.1.3 have inaccurate or incomplete **personal data** about them rectified

12.1.4 restrict **processing** of their **personal data**

12.1.5 have **personal data** we hold about them erased

12.1.6 have their **personal data** transferred

12.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure.

12.3 The Trusts Subject Access Request procedure can be found in appendix 1.

The Right to Object

12.4 In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.5 An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.6 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.7 In respect of direct marketing any objection to **processing** must be complied with.

12.8 The Oak Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

12.9 If a **data subject** informs The Oak Trust **personal data** held about them by The Oak Trust is inaccurate or incomplete then we will consider that request and provide a response within one month.

12.10 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

12.11 We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

12.12 **Data subjects** have a right to 'block' or suppress the **processing** of **personal data**. This means that The Oak Trust can continue to hold the **personal data** but not do anything else with it.

12.13 The Oak Trust must restrict the **processing** of **personal data**:

12.13.1 where it is in the process of considering a request for **personal data** to be rectified (see above)

12.13.2 where The Oak Trust is in the process of considering an objection to processing by a **data subject**

12.13.3 where the **processing** is unlawful but the **data subject** has asked The Oak Trust not to delete the **personal data**

12.13.4 where The Oak Trust no longer needs the **personal data** but the **data subject** has asked The Oak Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against The Oak Trust

12.14 If The Oak Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.15 The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

12.16 **Data subjects** have a right to have **personal data** about them held by The Oak Trust erased only in the following circumstances.

12.16.1 Where the **personal data** is no longer necessary for the purpose for which it was originally collected.

12.16.2 When a **data subject** withdraws consent – which will apply only where The Oak Trust is relying on the individuals consent to the **processing** in the first place.

12.16.3 When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object.

12.16.4 Where the **processing** of the **personal data** is otherwise unlawful.

12.16.5 When it is necessary to erase the **personal data** to comply with a legal obligation.

The Oak Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

12.16.6 to exercise the right of freedom of expression or information

12.16.7 to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law

12.16.8 for public health purposes in the public interest

12.16.9 for archiving purposes in the public interest, research or statistical purposes

12.16.10 in relation to a legal claim.

12.17 If The Oak Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.18 The DPO must be consulted in relation to requests under this right.

Right to Data Portability

12.19 In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.

12.20 If such a request is made then the DPO must be consulted.

13 Data security

13.1 We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.

13.2 We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction. Staff members of the Academy Trust should refer to the Information Security Policy for more detail.

13.3 Security procedures include:

13.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to a member of the Senior Leadership Team.

13.3.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

13.3.3 **Methods of disposal.** Paper documents should be shredded or placed in confidential waste sacks. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

13.3.4 **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

13.3.5 **Working away from the school premises – paper document.** If secure remote access if not possible, removal off site of Academy paper information assets containing personal data should only be done with authorisation which should include a risk assessment based on the criticality of the hard copy information. Staff members of the Academy Trust should refer to the Information Security Policy for more detail.

13.3.6 **Working away from the school premises – electronic working.** Academy staff working at home or remotely are responsible for ensuring that all Academy

information is kept confidential and secure to prevent access by a third party, and are required to adhere to all Information Security, Data Protection, Acceptable Use and other relevant policies. Information should not be transferred to client devices. Staff members of the Academy Trust should refer to the Information Security Policy for more detail.

13.3.7 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14 Data Protection Impact Assessments

14.1 The Oak Trust takes data protection very seriously, and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

14.3 The Oak Trust will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15 Disclosure and sharing of personal information

15.1 We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2 The Oak Trust will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared with the police in the investigation of a criminal offence.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

15.4 Further detail is provided in our Schedule of Processing Activities.

16 Data processors

16.1 We contract with various organisations who provide services to The Oak Trust, including:

16.1.1 Payroll providers, school meal providers, academic achievement and event providers and other supplier and service providers.

16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.3 **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of The Oak Trust. The Oak Trust will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 Contracts with **data processors** will comply with Data Protection Legislation and contain explicit obligations on the **data processor** to ensure compliance with the Data Protection Legislation, and compliance with the rights of **Data Subjects**.

17 Images and videos

17.1 Parents and others attending The Oak Trust events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Oak Trust does not prohibit this as a matter of policy.

17.2 The Oak Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of The Oak Trust to prevent.

17.3 The Oak Trust asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

17.4 As a Multi Academy Trust we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

17.5 Whenever a pupil begins their attendance at The Oak Trust they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

18 CCTV

18.1 The Oak Trust operates a CCTV system. Please refer to The Oak Trust CCTV Policy.

19 Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Appendix 1

Subject Access Request Procedure

1. Recognising a subject access request

1.1. As The Oak Trust **processes personal data** concerning **data subjects**, those **data subjects** have the right to access that **personal data** under Data Protection law. A request to access this personal data is known as a subject access request or SAR.

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

1.3. Any request by a **data subject** for access to their **personal data** is a SAR. This includes requests received in writing, by email, and verbally.

1.4. If any member of our **Workforce** receives a request for information they should inform the Data Protection Officer ("DPO") as soon as possible.

1.5. In order that the Trust is properly able to understand the nature of any SAR and to verify the identity of the requester, any requester making a request verbally should be asked to put their request in writing and direct this to the DPO.

1.6. A SAR will be considered and responded to in accordance with the Data Protection Law.

1.7. Any SAR must be notified to the DPO at the earliest opportunity.

2. Verifying the identity of a Requester

2.1. The Trust is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are.

2.2. Where the Trust has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two or more of the following:

2.2.1. Current passport
2.2.2. Current driving licence
2.2.3. Recent utility bills with current address
2.2.4. Birth/marriage certificate
2.2.5. P45/P60
2.2.6. Recent credit card or mortgage statement

2.3. If the Trust is not satisfied as to the identity of the requester then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of **personal data** resulting to a data breach.

3. Fee for Responding to Requests

3.1. The Trust will usually deal with a SAR free of charge.

3.2. Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively the Trust may refuse to respond to the request. If a request is considered to be

manifestly unfounded or unreasonable the Trust will inform the requester why this is considered to be the case.

3.3. 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.

4. Time Period for Responding to a SAR

4.1. The Trust has one month to respond to a SAR. This will run from the later of a. the date of the request, b. the date when any additional identification (or other) information requested is received, or c. payment of any required fee.

4.2. In circumstances where the Trust 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 (see below in relation to sharing information with third parties).

4.3. 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.

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

5. Form of Response

5.1. A requester can request a response in a particular form. In particular where a request is made by electronic means then, unless the requester has stated otherwise, the information should be provided in a commonly readable format.

6. Sharing Information with Third Parties

6.1. **Data subjects** can ask that you share their **personal data** with another person such as an appointed representative (in such cases you should request written authorisation signed by the **data subject** confirming which of their **personal data** they would like you to share with the other person).

6.2. Equally if a request is made by a person seeking the **personal data** of a **data subject**, and which purports to be made on behalf of that **data subject**, then a response must not be provided unless and until written authorisation has been provided by the **data subject**. The Trust should not approach the **data subject** directly but should inform the requester that it cannot respond without the written authorisation of the **data subject**.

6.3. If the Trust 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.

6.4. **Personal data** belongs to the **data subject**, and in the case of the **personal data** of a child regardless of their age the rights in relation to that **personal data** are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the **personal data** of their child.

6.5. However there are circumstances where a parent can request the **personal data** of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the Trust is confident that the child can understand their rights. Generally where a child is under 12 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their **personal data** on their behalf.

6.6. In relation to a child 12 years of age or older, then provided that the Trust 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 Trust will require the written authorisation of the child before responding to the requester, or provide the **personal data** directly to the child in accordance with the process above.

6.7. In all cases the Trust should consider the particular circumstances of the case, and the above are guidelines only.

7. Withholding Information

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

7.2. Where the information sought contains the **personal data** of third party **data subjects** then the Trust will:

7.2.1. Consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information;

7.2.2. If this is not possible, consider whether the consent of those third parties can be obtained; and

7.2.3. If consent has been refused, or it is not considered appropriate to seek that consent, then to consider whether it would be reasonable in the circumstances to disclose the information relating to those third parties. If it is not then the information may be withheld.

7.3. So far as possible the Trust will inform the requester of the reasons why any information has been withheld.

7.4. Where providing a copy of the information requested would involve disproportionate effort the Trust will inform the requester, advising whether it would be possible for them to view the documents at the Trust or seeking further detail from the requester as to what they are seeking, for example key word searches that could be conducted, to identify the information that is sought.

7.5. In certain circumstances information can be withheld from the requester, including a **data subject**, on the basis that it would cause serious harm to the **data subject** or another individual. If there are any concerns in this regard then the DPO should be consulted.

8. Process for dealing with a Subject Access Request

8.1. When a subject access request is received, the Trust will:

8.1.1. notify the DPO who will be responsible for managing the response and relevant department heads;

8.1.2. [subject to para 4.6 above,] acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days

8.1.3. take all reasonable and proportionate steps to identify and disclose the data relating to the request;

8.1.4. never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted;

8.1.5. consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;

8.1.6. seek legal advice, where necessary, to determine whether the Trust is required to comply with the request or supply the information sought;

8.1.7. provide a written response, including an explanation of the types of data provided and whether and as far as possible for what reasons any data has been withheld and;

8.1.8. ensure that information disclosed is clear and technical terms are clarified and explained.

Appendix 2

Data Breach Notification

1 About Data Breach Notification

1.1 This policy informs all of our **workforce** on dealing with a suspected or identified data security breach.

1.2 In the event of a suspected or identified breach, The Oak Trust must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

1.3 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

1.4 The Trust must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

1.5 Failing to appropriately deal with and report data breaches can have serious consequences for the Trust and for **data subjects** including:

1.5.1 identity fraud, financial loss, distress or physical harm;

1.5.2 reputational damage to the Trust; and

1.5.3 fines imposed by the ICO.

2 Identifying a Data Breach

2.1 A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

2.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

2.2.1 Leaving a mobile device on a train;

2.2.2 Theft of a bag containing paper documents;

2.2.3 Destruction of the only copy of a document; and

2.2.4 Sending an email or attachment to the wrong recipient; and

2.2.5 Using an unauthorised email address to access personal data; and

2.2.6 Leaving paper documents containing personal data in a place accessible to other people.

3 Internal Communication

Reporting a data breach upon discovery

3.1 If any member of our **workforce** suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our **workforce**, a **data processor**, or any other individual) then they must contact the Data Protection Officer ("the DPO") immediately at: Mrs Janet Eppleston (DPO), based at North Chadderton School, 0161 624 9939 extension 8025970. **Either in person or by telephone**. In her absence, you must contact Mrs Gillian Hindle, Senior Director, or Mrs Joy Clark, Headteacher and CEO.

3.2 The data breach may need to be reported to the ICO, and notified to **data subjects**. This will depend on the risk to **data subjects**. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

3.3 If it is considered to be necessary to report a data breach to the ICO then the Trust must do so within 72 hours of discovery of the breach.

3.4 The Trust may also be contractually required to notify other organisations of the breach within a period following discovery.

3.5 It is therefore critically important that whenever a member of our **workforce** suspects that a data breach has occurred, this is reported internally to the DPO immediately.

3.6 Members of our **workforce** who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

3.7 In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

***Breach minimisation**:*

3.8 The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any **personal data**. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

3.8.1 remote deactivation of mobile devices;

3.8.2 shutting down IT systems;

3.8.3 contacting individuals to whom the information has been disclosed and asking them to delete the information; and

3.8.4 recovering lost data.

***Breach investigation**:*

3.9 When the Trust has taken appropriate steps to minimise the extent of the data breach it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

3.10 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

3.10.1 what data/systems were accessed;

3.10.2 how the access occurred;

3.10.3 how to fix vulnerabilities in the compromised processes or systems;

3.10.4 how to address failings in controls or processes.

3.11 Other steps are likely to include discussing the matter with individuals involved to appreciate exactly what occurred and why, and reviewing policies and procedures.

***Breach analysis**:*

3.12 In order to determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform the Trust as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

3.13 Such an analysis must include:

3.13.1 the type and volume of **personal data** which was involved in the data breach;

3.13.2 whether any **special category personal data** was involved;

3.13.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

3.13.4 the security in place in relation to the **personal data**, including whether it was encrypted;

3.13.5 the risks of damage or distress to the **data subject**.

3.14 A breach notification form must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach. This will act as evidence as to the considerations of the Trust in deciding whether or not to report the breach.

4 External communication

4.1 All external communication is to be managed and overseen by the DPO and / Headteacher.

Law Enforcement

4.2 The DPO will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

4.3 DPO shall coordinate communications with any law enforcement agency.

Other organisations

4.4 If the data breach involves **personal data** which we process on behalf of other organisations then we may be contractually required to notify them of the data breach.

4.5 The Trust will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

Information Commissioner's Office

4.6 If the Trust is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then the Trust has 72 hours to notify the ICO if the data breach is determined to be notifiable.

4.7 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

4.7.1 the type and volume of **personal data** which was involved in the data breach;

4.7.2 whether any **special category personal data** was involved;

4.7.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

4.7.4 the security in place in relation to the **personal data**, including whether it was encrypted;

4.7.5 the risks of damage or distress to the **data subject**.

4.8 If a notification to the ICO is required then see part 5 of this policy below.

Other supervisory authorities

4.9 If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

4.10 When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects** then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by the Trust.

4.11 The communication will be coordinated by the DPO and will include at least the following information:

4.11.1 a description in clear and plain language of the nature of the data breach;

4.11.2 the name and contact details of the DPO;

4.11.3 the likely consequences of the data breach;

4.11.4 the measures taken or proposed to be taken by the Trust to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

4.12 There is no legal requirement to notify any individual if any of the following conditions are met:

4.12.1 appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);

4.12.2 measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

4.12.3 it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

4.13 For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

Press

4.14 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

4.15 All press enquiries shall be directed to Mrs Gillian Hindle, Senior Director of Business and HR.

5 Producing an ICO Breach Notification Report

5.1 All members of our **workforce** are responsible for sharing all information relating to a data breach with the DPO, which will enable the Notification Report Form to be completed.

5.2 When completing a Breach Notification Report Form all mandatory (*) fields must completed, and as much detail as possible should be provided.

5.3 The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

5.4 If any member of our **workforce** is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

5.5 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

5.6 The ICO requires that the Trust send the completed Breach Notification Form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

6 Evaluation and response

6.1 Reporting is not the final step in relation to a data breach. The Trust will seek to learn from any data breach.

6.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our **workforce** to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

ANNEX

DEFINITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Workforce	Includes any individual employed by *[School/Trust/Academy]* such as staff and those who volunteer in any capacity including governors [and/or trustees / members/ parent helpers].