Trust Data Protection Policy

Version	4.0
Approved By	Trustee Board
Issue Date	April 2018
Last Review Date	June 2023
Next Review Date	June 2024

REVIEW HISTORY

VERSION NO.	DATE OF CHANGE	CHANGE SUMMARY	REF
1.0	Sep 2019	Converted to Trust template. John Walker named as DPO	8
1.0	Feb 2021	Amendments based on DPO advice	
2.0	June 2021	Amendments based on DPO advice	
3.0	May 2022	Re-formatted title page	1
3.0	May 2022	Removed John Walker's email address and replaced with trust email address so he is not contacted directly	15
4.0	April 2023	Updated breach guidance (appendix 1) to differentiate between cyber breach and non and include Cyber security lead details	13/14

CONTENTS

Data Protection Policy

At Oak Multi Academy Trust we are committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data - and that is a personal responsibility that we take very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

Each school will be responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school.

The Trust central team are responsible for data held centrally about individuals.

Where we use the phrase 'we' that refers to the trust and the individual schools.

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the Data Protection Act 2018.

Oak Multi Academy Trust wants to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

Privacy Notices that explain how data about specific groups or activities is used and stored are also available. These can be obtained from each school and links on the website to UK GDPR compliance.

What are the key principles of the UK GDPR?

Lawfulness, transparency and fairness.

Oak Trust must have a legitimate reason to hold the data, this is explained in the Privacy Notices on our websites. To comply with the law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully. If you wish to withdraw consent, we have forms to complete to allow us to process your request which can be found on our website. There are sometimes when you cannot withdraw consent as explained in 'Data Subject's Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms. Initially an approach should be made directly to the individual school.

Retention

Oak Multi Academy Trust uses the Information and Records Management Society: Retention Guidelines for Schools with regard to how long records are stored. This is available on request.

Security

Oak Multi Academy Trust has processes in place to keep data safe including paper files, electronic records or other information detailed in a separate information security policy. Please see the following:

- CCTV Policy
- Online Safety Policy

Who is a 'data subject'?

Someone whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right: -

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for academies to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in academies.

Data subjects' rights are also subject to child protection and safeguarding concerns,

sharing information for the prevention and detection of crime. Academies also have legal and contractual obligations to share information with organisations' such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide for Data Subjects'.

Subject Access Requests (SARs)

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This Subject Access Request process is set out separately. You may need to provide identification evidence for us to process the request.

We must provide the information within a month, but this can be extended if, for example, the academy was closed for holidays. The maximum extension is up to two months.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal, or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g., school nurses who are employed by the NHS.

We will supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy and later information in this DPA policy.

Who is a 'data controller'?

The academy trust is the Data Controller. They have ultimate responsibility for how the schools and trust central team manage data. They delegate this processing to individuals to act on their behalf, that is the trust central team and the relevant school staff in each setting.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a Trustee, a contractor or temporary employee. It can also be another organisation such as the police or the Local Authority.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

Oak Multi Academy Trust must have a reason to process the data about an individual. Our privacy notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

The legal basis and authority for collecting and processing data in Oak Trust are:

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of:

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the academies
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities, and other specialist organisations may be used to determine whether data is shared.

Sensitive information must not be shared unless the person is authorised to receive it.

Any transfers of confidential information should be secure and the method risk assessed.

For electronic information transfers encrypted software should be used.

When information is requested by telephone it is important to:

- Ask the caller to confirm their name, job title, department and organisation and verify this by returning their call via their organisation's switchboard.
- Confirm the reason for the request.
- Be satisfied that disclosure of the requested information is justified.
- Place a record on the student / staff file noting the name of the person disclosing the information, the date and time of the disclosure, the reason for the disclosure, who authorised it (if applicable) and the recipient's details.

When sending personal or sensitive information by post:

- Check the name, department and address of the intended recipient.
- Use a robust envelope, clearly marked "PRIVATE & CONFIDENTIAL To be opened by the addressee only".
- Information to a service or department within the Local Authority should be sent using the internal post system.
- If the public post system is to be used a return address must be recorded on the outside of the envelope, and recorded delivery should be used if the information is highly sensitive.

Breaches & Non-Compliance

If there is non-compliance with the policy or processes, or there is a data breach, Oak Multi Academy has a separate procedure to follow to take immediate action to remedy the situation as quickly as possible.

Protecting data and maintaining data subjects' rights is the purpose of this policy and associated procedures.

Please see Appendix 1 for a copy of the Trust's Breach and Non-Compliance Procedure.

Consent

As a trust, where required, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

Consent is defined by the UK GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

This will largely be managed in individual schools.

Consent and Renewal

On the Oak Trust website are privacy notices that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important as well as ensuring the accuracy of that information.

For Pupils and Parents/Carers

On joining a school, you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in-school purposes, as set out on the data collection/consent form.

The contact and consent form is reviewed on an annual basis. It is important to inform the school if details or your decision about consent changes. A form is available. This is the obligation of each individual to notify the school of changes.

Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent

from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory, or regulatory constraints. Where more than one person can provide or withdraw consent, Oak Trust will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate form which can be found on the website

Associated Data Protection Policies

- CCTV
- Complaints
- Records Management Retention Guidelines

CCTV Policy

Please also see the CCTV policy. We use CCTV and store images for a period of time in line with the policy. CCTV may be used for:-

- Detection and prevention of crime
- School staff disciplinary procedures
- Pupil behaviour and exclusion management processes
- To assist the school in complying with legal and regulatory obligations

Data Protection Officer

We have a Data Protection Officer whose role is:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR
- to monitor compliance with the UK GDPR and DPA
- to provide advice where requested about the data protection impact assessment and monitor its performance
- to be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure

- to advise about training and CPD for the UK GDPR

Our DPO is John Walker whose contact details are:

Address:

6 Delamore Park | Cornwood | Ivybridge | PL21 9QP

Email: John.Walker@phplaw.co.uk

Physical Security

As a trust we are obliged to have appropriate security measures in place.

In school, every secure area has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

Equipment and paper files must not be left on view in any public setting.

Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons or members of the public.

Employees are expected to take appropriate measures to always ensure the security of personal data, including keeping records secure if visiting students in their homes.

The Premises Manager is responsible for authorising access to secure areas along with the SLT.

All Staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have the suitable security and review measures in place.

Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

All data, whether paper or electronic, must be disposed of properly and in accordance with the Trust's document retention and disposal schedule (found on the Trust website).

If a PC or laptop is to be given to another user, personal data should first be removed from it (e.g. student databases, free school meal information, etc).

PCs and laptops must be disposed of securely, through our current approved supplier

list.

It is imperative that staff follow any guidelines issued when overwriting data. Sending information to a computer's recycle bin does not delete the data as such. It is therefore important to empty the recycle bin regularly.

Paper records containing personal data or confidential information must be shredded.

These processes, when undertaken by a third party are subject to contractual conditions to ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)

The Trust Complaints Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the form, and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 12/24 months.

Appendix 1: Data Breach and Non-Compliance Procedure

All staff, governors and trustees must be aware of what to do in the event of a DPA / GDPR breach.

The 'Data Breach Flowchart' (Appendix 3) outlines the process. The 'Data Breach Form' will be completed and updated as the process progresses via the school GDPR Lead (details below). In the event of a cyber-criminal attack, you should inform your Cyber Security Lead who will complete an incident log and follow the correct procedures.

Most breaches, aside from cyber-criminal attacks, occur because of human error. They are not malicious in origin and if quickly reported are often manageable. Everyone needs to understand that if a breach occurs it must be swiftly reported.

What is a breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of breaches are: -

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its

records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter. Report the breach to the School GDPR Lead and Trust Governance Manager as soon as possible, this is essential. The Trust Governance Manager will liaise with the DPO and report any breaches to them.

Any cyber-criminal attacks will need to be reported to the school's Cyber Security Lead, details below. They will then inform the Managed Service Provider, AIT.

Trust Governance Manager: Danielle Benyon-Payne, admin@oaktrust.org T: 0116 303 3721

GDPR Leads

School	Name	Office hours	Out of hours
Brookside Primary School	Richard Skelton	0116 271 3680 / 201	07951498804
Manor High School	Bukie Ayo Bello Out of hours / Alison Dawes	0116 272 9799 / 799	07900922501
Overdale Infant School	Jenny Robinson	0116 2882724 / 415	07769654636
Overdale Junior School	Ravinder Kooner Out of hours: Sarah Cooke	0116 288 3736	07795573048
Woodland Grange Primary	Annette Howard / James Parker	0116 2720401 / 501	07482316089

Cyber Security Leads

Brookside Primary School	Richard Skelton	0116 271 3680 / 201	07951498804
Manor High School	Alison Dawes	0116 272 9799 / 799	07900922501
Overdale Infant School	Jenny Robinson	0116 2882724 / 415	07769654636
Overdale Junior School	Sarah Cooke	0116 288 3736/402	07795573048

Woodland Grange Primary	Annette Howard / James Parker	0116 2720401 / 501	07482316089

What happens next?

The breach notification form will be completed by the Trust Governance manager, and the breach register updated. Advice will be sought from the DPO. Consideration is given about how to effectively manage the breach, who to inform and how to proceed.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed.

The breach report will be within 72 hours of becoming aware of the breach. It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

In the event of a cyber incident, the insurance company will also be notified (appendix 4).

Procedure – Breach notification data controller to data subject

For every breach, the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk, they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Trust Governance Manager and DPO.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as

an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of Trust staff, which may be the Governance Manager, Managed Service Provider (for a cyber-attack) or Data Protection Officer, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

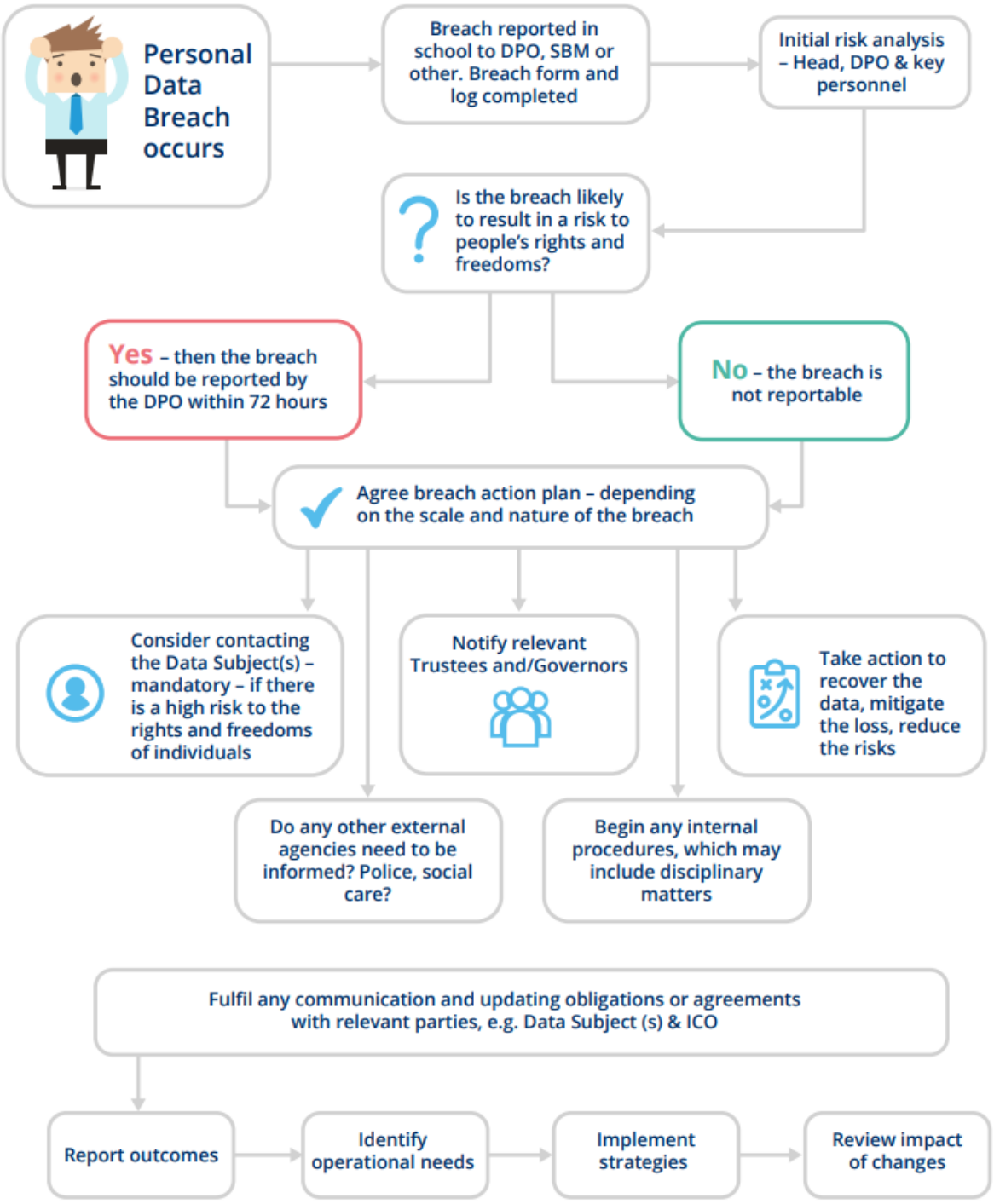
A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

Appendix 2 – Data Breach Reporting form including cyber incidents

Please send any information regarding a data breach to admin@oaktrust.org in the following format:

Date Reported	Date and Time of Breach	Notified by	Reported to	Description of Breach	Data subjects affected	proposed outcome

Appendix 3: Data Breach Flow Chart



Appendix 4: Insurance requirements in cyber incident