drb Ignite Multi Academy Trust

Data Protection Policy

Contents

1. Aim

The Trust's aim is to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the *Data Protection Act 2018* (DPA 2018) as set out in the Data Protection Bill.
This Policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This Policy meets the requirements of the GDPR and the expected provisions of the *Data Protection Act 2018*. It is based on guidance published by the *Information Commissioner's Office (ICO*) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the Trust's use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this Policy complies with the Trust's DfE *Funding Agreement* and *Articles of Association.*

3. Definitions

Personal data – any information relating to an identified or identifiable natural person ('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.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation.

Data Protection Officer (DPO) – the person in the Trust who determines the purposes and means of the processing of personal data.

Data subject – any individual who is the subject of personal data held by the Trust.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.

Profiling – any form of automated processing of personal data intended to evaluate certain personal aspects relating to a person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the Trust and supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means 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.

Child – the GDPR defines *a child* as anyone under the age of 16 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised by the Trust or decentralised at Trust schools.

4. The data controller

The Trust processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller. The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This Policy applies to **all staff** employed by the Trust and to external organisations or individuals working on the Trust's behalf. Staff who do not comply with this Policy may face disciplinary action.

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that the Trust and its school comply with all relevant data protection obligations.

5.2 Data Protection Officer

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

An *annual report* of related activities will be presented to the Trust Board and where relevant, report to the Board their advice and recommendations on Trust data protection issues.

The *Data Protection Officer* (DPO) is also the first point of contact for staff on all GDPR issues and for the ICO.

The Trust's DPO is Alvin Walters email: dpo@drbignitemat.co.uk

5.3 CEO and headteachers

The Trust's CEO and headteachers act as representatives of the data controller on a day-to-day basis.

5.4 Staff

Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this Policy
- informing the Trust/school of any changes to their personal data e.g. a change of address
- familiarising themselves with the data protection principles in *Section 6* below.
- contacting the DPO:
    - with any questions about the operation of this Policy, data protection law, retaining personal data or keeping personal data secure
    - if they have any concerns that this Policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the Trust
    - if there has been a data breach in which case the DPO ***MUST*** be informed immediately
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - if they need help with any contracts or sharing personal data with third parties.

6. Data protection principles and DPO

The GDPR is based on data protection principles that the Trust must comply with.

The principles state that personal data must be:

- **Processed lawfully, fairly and in a transparent manner.**

  For note:

  Lawful – means identifying a lawful basis before personal data can be processed. These are often referred to as the *conditions for processing* and include such things as consent.

  Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects.

  Transparently – the GDPR includes rules on giving privacy information to data subjects These are detailed and specific and place an emphasis on making privacy notices

understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The ICO provides further guidance on privacy notices, transparency and control here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

- **Purpose and intent of processing**

Personal data can only be obtained for *specified, explicit and legitimate processing purposes* the data subject has been made aware of and no other without further consent.

- **Data minimisation**

Data collected on the data subject should be limited to what is necessary in relation to the purposes for which it is processed.

- **Accurate and up to date**

The data controller must ensure as far as is reasonably possible that the information collected is correct and current.

- **Retention limitations**

All personal information ***MUST*** have an expiration date applied appropriate to its collected purpose, after which it must cease to be available

- **Security**

Processors must ensure appropriate technical and organisational measures are in place to ensure data security. This includes protection against unlawful processing, accidental loss, destruction or damage.

The Data Protection Officer

The *Data Protection Officer* will carry out risk assessments taking into account all the circumstances of the Trust's controlling or processing operations.

In determining appropriateness, the *Data Protection Officer* will consider the extent of possible damage or loss that might be caused to individuals if a security breach occurs, the effect of any security breach on the Trust itself and any likely reputational damage including the possible loss of stakeholder trust.

When assessing appropriate **technical** measures, the *Data Protection Officer* will consider such operational behaviours as:

- Password protection
- Automatic locking of idle terminals
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of devices that leave Trust premises such as laptops

- Security of all networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation
- Implementing appropriate security standards relevant to the Trust.

When assessing appropriate **organisational** measures the *Data Protection Officer* will consider the following:

- The appropriate training levels throughout Trust
- Measures that consider the reliability of staff e.g. such as job references
- The inclusion of *data protection* expectations in staff contracts
- Identification of disciplinary action measures for data breaches
- Monitoring of staff for compliance with relevant security standards
- Physical access controls to electronic and paper-based records
- Adoption of a clear desk policy
- Storing of paper-based data in lockable fire-proof cabinets
- Restricting the use of portable electronic devices outside of the workplace
- Restricting the use of staff's own personal devices being used in the workplace
- Adopting clear rules about passwords
- Making regular backups of personal data and storing the media off-site
- The imposition of appropriate security measures when transferring data outside the Trust.

For note:
The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires the DPO to demonstrate compliance with the principles and states explicitly that this is the responsibility of the DPO.

The ICO has published guidance on accountability and governance which can be viewed here:

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

The Trust will only process personal data where it can demonstrate one of *6 lawful bases* i.e. legal reasons to do so under data protection law:

- The data needs to be processed so that the Trust/school can ***fulfil a contract*** with the individual, or the individual has asked the Trust/ school to take specific steps before entering into a contract
- The data needs to be processed so that the Trust/school can ***comply with a legal obligation***
- The data needs to be processed to ensure the ***vital interests*** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust/school can perform a task in the ***public interest*** and thereby carry out its official functions

- The data needs to be processed for the ***legitimate interests*** of the Trust/school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For note:
For special categories of personal data, the Trust will also meet one of the special category conditions for processing which are set out in the *GDPR* and *Data Protection Act 2018*.

7.2 Limitation, minimisation and accuracy

The Trust will only collect personal data for specified, explicit and legitimate reasons. The Trust will explain these reasons to individuals when their data is first collected. If the Trust wants to use personal data for reasons other than those given when the data is first obtained, it will inform the individuals concerned before it does so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their job.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's *Retention of Records Procedure* and *Retention of Records Schedule*.

8. Sharing personal data

The Trust will not normally share personal data with anyone else. However, there may be exceptions where:

- there is an issue with a pupil or parent/carer that puts the safety of staff at risk
- there is need to liaise with other agencies. The Trust/school will seek consent as necessary before doing this
- Trust suppliers or contractors need data to enable them to provide services to our staff and pupils. When doing this the Trust will:
    - only appoint suppliers or contractors who can provide sufficient guarantees that they comply fully with data protection law
    - establish a *data sharing agreement* with the supplier or contractor, either in the contract or as a stand-alone agreement, to ensure the fair and lawful processing of any personal data the Trust shares
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust.

The Trust will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention or detection of crime and/or fraud
- the apprehension or prosecution of offenders
- the assessment or collection of tax owed to HMRC
- in connection with legal proceedings
- where the disclosure is required to satisfy safeguarding requirements

- research and statistical purposes, as long as personal data is sufficiently anonymised, or full consent has been provided.

For note:
The Trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of the Trust's pupils or staff.
Where the Trust transfers personal data to a country or territory outside the *European Economic Area*, it will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a ***subject access request*** to gain access to personal information that the Trust/school holds about them.

This includes:

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of any data processing
- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored, or if this isn't possible, the criteria used to determine this period
- the source of the data, if not the individual
- whether any automated decision-making is being applied to the data and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the Trust's DPO.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If senior leaders receive a ***subject access request*** they must immediately forward it to the Trust DPO and follow the Trust's Subject Access Request Procedure (GDPR DOC 2.2).

9.2 Children and subject access requests

Personal data about a child belongs to that child and not the child's parents or carers. For a parent or carer to make a *subject access request* with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a *subject access request*. Therefore, most subject access requests from parents or carers of pupils in Trust schools may be granted without the express permission of the pupil.

For note:
This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to subject access requests the Trust:

- may ask the individual to provide 2 forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request
- will provide the information free of charge
- may tell the individual it will comply within 3 months of receipt of the request, where a request is complex or numerous. The Trust will inform the individual of this within 1 month, and explain why the extension is necessary

The Trust will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, the Trust may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When the Trust refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request and to receive information when the Trust is collecting their data about how the data will be used and processed, individuals also have the right to:

- withdraw their consent to processing at any time
- ask the Trust to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing

- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the *European Economic Area*
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the Trust's DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see their child's educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes a range of information about a pupil) within 15 school days of receipt of a written request.

11. Biometric recognition systems

Where the Trust uses pupils' biometric data as part of an automated biometric recognition system e.g. pupils use finger prints to receive school dinners instead of paying with cash, the Trust will comply with:

- the requirements of the Protection of Freedoms Act 2012
- Article 9 of the GDPR
- the Trust Biometric Data Policy

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust/school will obtain written consent from at least one parent or carer before it takes any biometric data from their child.

Parents/carers and pupils have the right to choose not to use any biometric system(s). The Trust/school will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in any biometric recognition system(s), or withdraw consent, at any time, and the Trust/school will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the Trust/school will not process that data irrespective of any consent given by the pupil's parents/carers.

12. CCTV

The Trust uses CCTV in various locations around school sites to maintain safety and security. The Trust will adhere to the ICO's code of practice for the use of CCTV.

The Trust does not need to ask individuals' permission to use CCTV, but it will make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about CCTV systems should be directed to the headteacher or DPO.

13. Photographs and videos

As part of Trust/school activities, photographs and record images of individuals may be taken within our schools.

The Trust/school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The Trust/school will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- within schools on notice boards and in school magazines, brochures, newsletters, etc.
- outside schools by external agencies such as the school photographer, newspapers, campaigns
- online on Trust/school websites or social media pages.

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

When using photographs and videos in this way the Trust/school will not accompany them with any other personal information about the child, to ensure they cannot be identified.

For note:
More information can be found in the Trust's *Safeguarding and Child Protection Policy*.

14. Data protection by design and default

The Trust will put measures in place to show that it has integrated data protection into all data processing activities including:

- appointing a suitably qualified DPO and ensuring the DPO has the necessary resources to fulfil all duties and maintain expert knowledge
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in Section 6
- completing *privacy impact assessments* where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Trust's DPO will advise on this process)
- integrating data protection into internal documents including this Policy, any related policies and associated privacy notices

- regularly training staff on data protection law, this Policy, any related policies and any other data protection matters
- regularly conducting reviews and audits to test Trust privacy measures and ensure full compliance with all GDPR requirements
- maintaining records of processing activities including:
    - for the benefit of data subjects, making available the name and contact details of the Trust and DPO and all information the Trust is required to share about how it uses and processes personal data via associated privacy notices
    - for all personal data that the Trust holds, maintaining an internal record of the type of data, data subject, how and why the Trust is using the data, any third-party recipients, how and why the Trust is storing the data, retention periods and how the Trust is keeping the data secure.

15. The Children's Code

The Children's code does not apply to schools.

To be defined as an *Information Society Service (ISS*), organisations must meet several qualifying conditions which are set out in services covered by the code. Schools do not meet the definition of an ISS. However, the Code's vision – to ensure that the best interests of children are a primary concern when using their data – closely aligns with the Trust's own educational mission.

The Trust/schools are required to comply with UK GDPR and the Data Protection Act 2018, and the Code sets out what good practice compliance looks like in the areas it covers. The Trust, therefore, aspires to meet the code's 15 standards as a matter of good practice.

Whilst the code does not apply to schools, wider UK data protection law does.

The Trust and its schools have a range of important responsibilities under the *UK GDPR* and the *DPA 2018* when procuring *EdTech service*s. These include, due diligence, safeguarding and oversight. The *UK GDPR* states that data protection by design should be taken into consideration for public tenders, and encourages organisations including Trusts and schools to make sure that controllers and processors are able to fulfil their data protection obligations' when selecting services.

The Trust considers carefully the responsibilities it and the EdTech provider will hold under a specific contractual agreement. More specifically, the degree to which the EdTech provider will be able to influence how children's data is used. The Trust considers who is acting as a sole data controller, or whether it is a joint controllers and processors.

For note:
Controllers and processors guidance gives more information to assist organisations to make this assessment.

If EdTech providers fulfil controller responsibilities, the Trust will make sure that EdTech providers are not defined as processors. Controller responsibilities include determining the means and purposes of data processing

Where an EdTech provider and the Trust are acting as joint controllers, the contract will define who is responsible for complying with different data protection requirements, although both are ultimately accountable for meeting them.

Even where an EdTech provider is acting as a processor, they still have legal obligations to assist the Trust as the controller. The Trust will remind EdTech processors of these obligations, which may include:

- maintaining a record of children's data processing activities, and ensuring they have not processed children's data in any way beyond the Trust's instruction
- proactively notifying the Trust without undue delay if there has been a personal data breach
- implementing appropriate security measures and safeguards to protect children's data
- assisting the Trust with its obligation to undertake *Data Protection Impact Assessments*

For note:
The Code applies to EdTech services that are likely to be accessed by children on a direct-to-consumer basis. These are services which are freely and directly available to users on open platforms such as the web or via an app store.
This is because EdTech providers meet all the criteria that define a relevant ISS in-scope of the code.

The Code applies even where the organisation providing the direct-to-consumer EdTech service operates on a non-profit basis.This is because most similar services are normally provided on a for-profit basis in the direct-to-consumer EdTech market, meaning non-profit EdTech are still considered *normally provided for remuneration* - part of the definition of being a relevant ISS.

The code also applies to EdTech services in another scenario. This is where an EdTech service is provided to children through a school, and the EdTech provider influences the nature and purpose of children's data processing.

Examples of where this is likely to apply include:

- schools procuring *off-the-shelf*, pre-defined, EdTechproducts,
- EdTech providers processing children's data for product development or research - where the research isn't the core service procured by a school
- EdTech providers processing children's data for marketing and advertising, or their own commercial purposes.

The Trust and EdTech provider will consider respective roles and responsibilities in order to determine whether the EdTech provider is acting as a joint controller or independent controller. Guidance on Controllers and processors provides more information.

The Children's Code applies here as the EdTech service meets all three criteria of the ISS definition.

For note:
The Trust will make sure EdTech providers comply with the following data protection principles:

- **Necessity and proportionality.** EdTech providers should be able to evidence that their use of children's data is effective in delivering the stated educational benefit
- **Purpose limitation**. Data gathered and processed by EdTech providers to fulfil the educational functions of the Trust must not be used for any other purpose. This includes re-using children's data for commercial gain, for example through advertising, research for commercial strategy, or new product development.
- **Lawful bases.** The "public task" lawful basis must not be used for data processing that doesn't relate to schools' public tasks, as defined by law (for example within the Education Act 2002). Where EdTech providers are processing for broader purposes, it is likely that legitimate interest legal basis is more appropriate.
- **Data minimisation.** Only gather or process children's data that is needed to perform the given educational function.
- **Data protection impact assessments**. Any processing likely to result in a high risk requires a DPIA – we consider any online service likely-to-be -accessed by children high risk, so EdTech services will need to work in partnership with schools to complete and regularly review a DPIA in respect of service being provided.

16. Data security and storage of records

The Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- papers containing confidential personal data ***must*** not be left on office or classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- where personal information needs to be taken off site, staff must sign it in and out from the school office
- passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the Trust's *Acceptable Use Policy*.
- Where the Trust needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

17. Disposal of records

Personal data that is no longer needed will be disposed of securely and in line with the Trust's Data Retention Policy. Personal data that has become inaccurate or out of date will also be disposed of securely, where the Trust cannot or does not need to rectify or update it.

For example, the Trust/school will shred or incinerate paper-based records and overwrite or delete electronic files. The Trust/school may also use a third party to safely dispose of records. The third party will be required to provide sufficient guarantees around compliance with data protection law.

18. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the DPO will follow a set procedure. When required, the DPO will report the data breach to the ICO within 72 hours. Such breaches in a Trust/school context may include, but are not limited to:

- anon-anonymised dataset being published on the Trust/school website which shows the test results of pupils eligible for the pupil premium
- safeguarding information being made available to an unauthorised person
- the theft of a Trust/school laptop containing non-encrypted personal data about pupils

19. Training

All staff and trustees are provided with data protection and cyber security training as part of their induction process. Data protection training will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

20. Publication of Information

All public authorities, including schools, are required under the *Freedom of Information Act* to adopt a publication scheme that has been approved by the *Information Commissioner*.

There is currently one approved model publication scheme, which has been produced by the *Information Commissioner's Office (ICO).*

The Trust has adopted the ICO's model scheme. For more information follow the link:

https://ico.org.uk/media/for-organisations/documents/1153/model-publication-scheme.pdf

21. Links with other policies

This Policy is linked to other Trust policies and GDPR requirements:

- Acceptable ICT Use Policy
- Information Security Policy

- User Access Management Policy
- Password Policy
- Biometric Data Policy
- ICO CCTV Code of Practice
- ICO Guidance on Personal Data Breaches
- Children's Code

Monitoring and review

The Trust's *Data Protection Officer* is the owner of this Policy and is responsible for ensuring it is reviewed in line with the review requirements of the GDPR.

The Policy is available to staff and parents on the Trust website.

Monitoring and review	DPO
Links	Health & Safety Policy and Procedures
Staff responsible	CEO DPO
Committee responsible	**Audit and Risk Committee**
Date approved by Trust Chair	 Date: Sept 2021
Reviewed	**September 2021**
Next review date	**September 2023**

For note:
Should there be any changes/further national guidance issued relevant to this Policy, it will be updated accordingly prior to the review date shown above and referred to the next Trust Board meeting.

Change history record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Richard Martin	1/5/2018
2	Updated section 10	Richard Martin	22/5/2018
3	Full review and Children's Code added	David Sheldon	14/9/2021

APPENDIX
TRUST DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Trust DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher, CEO and Trust Chair as appropriate
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff or data processors where necessary
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  For note:
  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in GDPRiS.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:

        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - facts and cause
    - effects
    - action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored in the Trust's GDPRiS Online Management System which is fully GDPR compliant.

- The DPO, CEO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

The Trust will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The Trust will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT Team to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure the Trust receives a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, the Trust will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If the sensitive/special category information/data was sent via an encrypted email solution, the encryption will be changed so that access to the email is revoked.
- If details of pupil premium interventions for named children are inadvertently published on the Trust/school website, the webpage in question will be updated without undue delay
- If non-anonymised pupil test results or staff pay information were shared with trustees, the DPO will be ask the trustees to return it
- A school laptop, smart phone or tablet containing non-encrypted sensitive personal data being stolen or hacked the IT team will be informed without undue delay and instructed to remotely wipe the laptop of all data
- If the school uses a cashless payment provider and it has been hacked resulting in parents' financial details stolen, the DPO will communicate this breach to all affected subjects and instruct them to inform their bank, credit card provider to block access to the affected bank account or credit/debit card