Marches Academy Trust

Date of last review: **March 2021**
Approved: **March 2021**
Date of next review: **September 2021**

Data Protection Policy (GDPR)

www.marchesacademytrust.co.uk

Contents

1. Aims

The Marches Academy Trust (the Trust) and its Schools aim to ensure that all personal data collected about staff, pupils, parents, governors, 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 DPA 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 our 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 regulation 5 of the Education (Pupil Information) (England) (Amendment) Regulations 2018
which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and Articles of Association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ▪ Name (including initials) ▪ Identification number ▪ Location data ▪ Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special categories of personal data	Personal data which is more sensitive and subsequently requires more protection, including information about an individual's: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious or philosophical beliefs ▪ Trade union membership ▪ Genetics ▪ Biometrics (such as fingerprints), where used for identification purposes ▪ Health – physical or mental ▪ Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Trust and its Schools processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a Data Controller.

The Trust and its Schools are 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 its Schools and to external organisations or individuals working on behalf of the Academy Trust and its Schools. 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 each School complies 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 our compliance with data protection law and developing related policies and guidelines where applicable.

They will provide an annual report of their activities to the Trustees Audit & Risk committee and, where relevant, report to the board their advice and recommendations on school data protection issues.

The Data Protection Officer is also the first point of contact for individuals whose data the Trust and its Schools processes and for the ICO.

The DPO is responsible for informing and advising schools on GDPR compliance, co-ordinating the response to incidents and managing relationships with supervising bodies as and when required.

The Trust Data Protection Officer is Howard Prince prince.h@sjt.mmat.org.uk

5.3 Headteacher/Head of School

The **Headteacher/Head of School** acts as the representative of the Data Controller.

5.4 **All staff** are responsible for:

- collecting, storing and processing any personal data in accordance with this Policy.
- informing the Trust and its Schools of any changes to their personal data, such as a change of address.
- contacting the DPO in the following circumstances:
  - 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, or if they are unsure whether 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 UK or if there has been a data breach.
- 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

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

The principles say that personal data must be:

- processed lawfully, fairly and in a transparent manner.
- collected for specified, explicit and legitimate purposes.
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- accurate and where necessary, kept up to date.
- kept for no longer than is necessary for the purposes for which it is processed.
- processed in a way that ensures it is appropriately secure.

This policy sets out how the Trust and its Schools aims to comply with these principles.

7. Collecting personal data

7.1. Lawfulness, fairness and transparency

The Trust and its Schools will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- the data needs to be processed so that the Trust and its Schools can fulfil a contract with the individual, or the individual has asked the Trust and/or its Schools to take specific steps before entering into a contract.
- the data needs to be processed so that the Trust and/or its Schools 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 and its Schools, as a public authority, can perform a task in the public interest and carry out its official functions;
- the data needs to be processed for the legitimate interests of the Trust and its Schools 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 special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps. and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

If we offer online services to pupils, such as classroom apps. and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2. Limitation, minimisation and accuracy

The Trust and its Schools will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

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 Information and Records Management Society toolkit for schools.

8. Sharing personal data

The Trust and its Schools will not normally share personal data with anyone else but may do so where:

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

The Trust and its Schools 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 our safeguarding obligations.
- research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

The Trust and its Schools may also share personal data with emergency services and Local Authorities, to help them to respond to an emergency that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the United Kingdom, we 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 and its Schools holds about them. This includes:

- confirmation that their personal data is being processed.
- access to a copy of the data.
- the purposes of the data processing.
- the categories of personal data concerned.
- with whom the data has been or will be shared.
- how long the data will be stored for 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 their data and what the significance and consequences of this might be for the individual.

Subject access requests should include:

- name of individual.
- correspondence address.
- contact number and email address.
- details of the information requested.

If staff receive a subject access request, they must immediately forward it to the DPO.

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.

Primary Schools

Children below the age of 12 are generally not considered to be sufficiently 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 at our Primary Schools, may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Secondary Schools

Children aged 12 and above are generally regarded as being sufficiently 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 at our Secondary Schools may not be granted without the express permission of the pupil. 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 requests we:

- will request the individual to provide two forms of identification.
- may contact the individual via telephone to confirm the request was made.
- will respond within one month of receipt of the request.
- will provide the information free of charge.
- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

The Trust and its Schools 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, we may refuse to act on it, or charge a reasonable fee which recognises 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 we refuse a request, we 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 (see above) and to receive information when we are collecting their data about how we use and process it, (see

section 7), individuals also have the right to:

- withdraw their consent to processing at any time.
- ask us 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 United Kingdom.
- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

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

11. Biometric recognition systems

Where the Trust and its Schools use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012

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 and its Schools will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

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

Parents/carers and pupils can object to participation in the biometric recognition system(s) or withdraw consent at any time and we 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, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time and the Academy will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the Trust and its Schools to ensure safety. We will adhere to the ICO's code of practice for the use of CCTV.

The Trust and its Schools do not need to ask individuals' permission to use CCTV, but we 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 the CCTV system should be directed to Howard Prince, prince.h@sjt.mmat.org.uk

13. Photographs and videos

As part of our normal school activities, we may take photographs and record images of individuals within our Trust and its Schools.

Primary Schools

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

Secondary Academies

The Trust's Secondary Schools will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

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

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

14. Data protection by design and default

The Trust and its Schools will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- appointing a suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their 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 relevant data protection law (see section 6).
- completing privacy impact assessments where the Trust and its Schools process personal data which presents a high risk to rights and freedoms of individuals and when introducing new technologies (the DPO will advise on this process).
- integrating data protection into internal documents including this policy, any related policies and privacy notices.
- regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - for all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Data security and storage of records

The Trust and its Schools 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 and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- passwords that are at required to be changed on a regular basis are used to access school computers, laptops and other electronic devices.
- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices;

- where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (section 8).

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trust and its Schools behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The Trust and its Schools will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- a non-anonymised dataset being published on the Trust and/or Schools Trust websites which shows the exam results of pupils eligible for the pupil premium.
- safeguarding information being made available to an unauthorised person.
- the theft of a Trust and/or its Schools laptop containing non-encrypted personal data about pupils.

18. Training

All staff, Trustees and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust and its Schools processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed on an annual basis.

20. Appendix 1 Personal 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 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 or altered.
  - Disclosed or made available where it should not have been to unauthorised people.
- The DPO will alert the Headteacher/Head of school and/or the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are and how likely they are to happen.
- The DPO will consider 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 or financial loss.
  - unauthorised reversal of pseudonymisation (for example, key-coding); damage to reputation or loss of confidentiality.
  - any other significant economic or social disadvantage to the individual(s) concerned If it is 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 later challenged by the ICO or an individual affected by the breach. Documented decisions are stored by the DPO.
- 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 or effects of 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 by the DPO.
- The DPO and Headteacher/Head of School 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 and its Schools 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 and its Schools 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.
- Members of 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 department 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 we receive 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, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach could include

- details of pupil premium interventions for named children being published on the Trust or School website.
- non-anonymised pupil exam results or staff pay information being shared with Governors.
- a Trust laptop containing non-encrypted sensitive personal data being stolen or hacked.
- the Trusts cashless payment provider being “hacked” and parents’ financial details stolen.

21. Appendix 2 Subject Access Request Form

General Data Protection Regulations
Right of Access to Personal Data

SUBJECT ACCESS REQUEST FORM

Information

We should respond to your request within one calendar month. Note this can be extended for a further two months if the request is deemed complex. However, this period does not start until:

a) We are satisfied about your identity

b) You have provided enough detail to locate the information you are seeking

Please complete the following sections of this form providing as much information as possible to help us deal with your request.

1. Provide details of the person about whom the Trust and/or its Schools is holding data (the Data Subject)

Full Name (Print) _____

Date of Birth _____

Present Address:	Previous Address (if less than 3 years at your present address):
Post Code:	Post Code:

Telephone Number _____

Email address _____

2. Are you requesting information about yourself (person referred to in question 1)?
If **YES**, then go to question 3. If **NO** please complete the following:

Full Name (Print

Present Address

Post Code

Telephone number

Email address

Relationship with data subject and brief explanation as to why you are requesting this information rather than the data subject:

_____

_____

If you are acting on behalf of the data subject you will need to enclose their written authority including a signature or other legal documentation (e.g. power of attorney) to confirm this request. You also need to enclose evidence of your identity and that of the data subject (see section 4 for details of acceptable identity)

3. Please provide a clear description of the information that you are requesting, see table below. **If you provide <u>specific</u> details of what information you want, e.g. name of a document relevant to a time period rather than just the whole of your file you may receive a quicker response.**

Description of Information	School holding this Information	Time Period for Information Requested

4. Please provide **two original documents** as evidence of your identity (one containing a photo). Acceptable types of documents used to verify your identity are detailed below.

Driving Licence	Passport	National ID Card	Medical Card	Utility Bill

You may wish to send your documents by special or recorded delivery. Your proof of identity will be returned to you securely after verification.

5. All information in respect to your request will be sent to you via secure email unless alternative arrangements are made. We may require further evidence of your identity if you collect your information from School premises.

Declaration

To be completed by all applicants. Please note that any attempt to mislead the The Marches Academy Trust and its Schools may lead to prosecution.

I (insert name) _____

_____

certify that the information given on this application form and any attachments therein to The Marches Academy Trust and/or its Schools is accurate and true.

I understand that it is necessary for The Marches Academy Trust and/or its Schools to confirm my identity and it may be necessary to obtain more information, in order to locate the requested information.

Signature _____

Date _____

Return of the Form

If you are either posting your documents or hand delivering them then our address is detailed below:

For the Attention of the Data Protection Officer
Howard Prince
Marches Academy Trust
Sir John Talbot's School
Prees Road
Whitchurch
SY13 2BY

Our email address is: prince.h@sjt.mmat.org.uk

How we will send you the information you have requested

We want you to receive the information you have requested in the most convenient way for you.

However, we do have an obligation under the General Data Protection Regulations to provide you with the information you have requested in the most secure way possible.

We believe the most secure way to provide you with the information is either:

- For you to collect the documentation in person from our offices
- For us to email you the information securely/encrypted

We can post your information to you but there are risks attached to providing you with your information using this method, eg your information may be lost by the delivery service or delivered to the wrong address.

Please confirm you are happy to receive your information by secure email by ticking the box below and confirming the email address that your information should be sent to:

Tick Box		Email address	

Alternatively, if you prefer any of the other methods below please indicate which by ticking ONE of the boxes below:

Collection in person		CD or Paper Copy *(please circle your choice)*

By Post (special delivery)		CD or Paper Copy *(please circle your choice)*

DOCUMENT CONTROL	
Policy owner	Data Protection Officer
Scope	All staff, Trustees and Governors
Last updated	March 2021
Effective from	March 2021
Next planned review	September 2021
Status	Approved
Date approved	10.03.2021
Summary of last revision	Updated in line with GDPR legislation
Related Policies	ICT policy