Data Protection Policy

1. Contents

2. Version control

Date	Version	Revision	Owner
Oct 2015	1.0	New Policy	Future Generation Trust Policy Team
24/05/18	2.0	Updated policy in-line with requirements of the GDPR	Future Generation Trust Policy Team
07/01/21	3.0	Scheduled policy review	Future Generation Trust Policy Team
10/03/23	4.0	Inclusion of Moat Hall Primary Academy and section on cloud computing	Future Generation Trust Policy Team

3. Policy statement

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

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

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

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

We will:

- Ensure that there is a single point of contact with the overall responsibility for data protection (the Data Protection Officer)
- Ensure each academy has a named Data Protection Lead
- Provide clarity with regard to responsibility and supervision to ensure compliance with Data Protection Legislation
- Carry out regular checks to monitor compliance with this policy across all academies

4. Legal framework

This policy has been developed using the Browne Jacobson GDPR toolkit for schools and has due regard to legislation and guidance, including, but not limited to the following:

- Data Protection Act (2018) and The UK General Data Protection Regulation (GDPR)
- DfE Data Protection toolkit for schools (2018)

This policy has due regard to the Trust's policies and procedures, including, but not limited to:

- Business Continuity Plans
- CCTV Policy
- Child Protection & Safeguarding Policy
- Data Breach Notification Policy
- E-Safety Policy
- Network and IT Security Policy
- Privacy Notices
- Protection of Biometric Information Policy
- Records Management Policy
- Subject Access Request Procedure

5. About this policy

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

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

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

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

6. Definition of data protection terms

All defined terms in this policy are indicated in bold text, and a list of definitions is included in Appendix A.

7. Data Protection Officer

As a multi-academy trust we are required to appoint a **Data Protection Officer** ("DPO").

Our DPO is **Stuart Ayres** (Chief Executive Officer), and they can be contacted at Future Generation Trust Office, Hobnock Road, Essington, Wolverhampton, WV11 2RF. Tel: 01922 496570 , or e-mail: office@futuregenerationtrust.co.uk

Future Generation Trust are registered with the Information Commissioner's Office (ICO) and have named the DPO as part of the registration process.

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

The DPO is also the central point of contact for all **data subjects** and others in relation to matters of data protection. Our network of academy-based Data Protection Leads (DPL) work closely with the DPO and individual academy queries should first be raised with the appropriate DPL.

The Data Protection Lead for each academy is:

Etching Hill CE Primary Academy	Zoe Hasketh-Boston	Business Manager
Gentleshaw Primary Academy	Nikkie Boston	Office Manager
Moat Hall Primary Academy	Kate Hutton	Office Support Manager
St John's Primary Academy	Laura Greenhouse	PA to the Headteacher
St Peter's CE Primary Academy	Rosie Chandler	Bursar

8. Data protection principles

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

- **Processed** fairly and lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- **Processed** securely using appropriate technical and organisational measures.

Personal Data must also:

- be **processed** in line with **data subjects'** rights;
- not be transferred to people or organisations situated in other countries without adequate protection.

We will comply with these principles in relation to any **processing** of **personal data** by the multi-academy trust.

9. Fair and lawful processing

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

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

- that the **personal data** is being **processed**;
- why the **personal data** is being **processed**;
- what the lawful basis is for that **processing** (see below);
- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

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

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

- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
- where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest; and
- where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**.

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

- where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
- where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;

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

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

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

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

Vital Interests

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

Consent

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

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

When pupils and or our **workforce** join the multi-academy trust a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate third parties may also be required to complete a consent form.

In relation to all pupils attending our primary academy's we will seek consent from an individual with parental responsibility for that pupil.

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

- Inform the **data subject** of exactly what we intend to do with their **personal data**;

- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and

- Inform the **data subject** of how they can withdraw their consent.

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

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

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

10. Processing for limited purposes

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

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

11. Notifying data subjects

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

- our identity and contact details as **data controller** and those of the DPO;
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**;
- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the UK and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to our **Records Management Policy**;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
- the rights of the **data subject** to object to or limit **processing**, request information, request deletion of information or lodge a complaint with the ICO.

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

Please note that for reasons of practicality, we request that parents and carers only provide additional emergency contact details for their child for third parties (e.g. relatives and friends) that acknowledge that our multi-academy trust will retain their personal data and have given their consent.

12. Adequate relevant and non-excessive

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

13. Accurate data

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

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

Data subjects have a right to have any inaccurate **personal data** rectified. See section 15 in relation to the exercise of this right.

14. Timely processing

We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required. For more information please refer to the Trust's **Records Management Policy**.

15. Processing in line with data subject's rights

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

- request access to any **personal data** we hold about them;
- object to the **processing** of their **personal data,** including the right to object to direct marketing;
- have inaccurate or incomplete **personal data** about them rectified;
- restrict **processing** of their **personal data**;
- have **personal data** we hold about them erased;
- have their **personal data** transferred; and
- object to the making of decisions about them by automated means.

The Right of Access to Personal Data

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

The Right to Object

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

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

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

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

The multi-academy trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

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

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

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

The Right to Restrict Processing

Data subjects have a right to "block" or suppress the **processing** of **personal data**. This means that the multi-academy trust can continue to hold the **personal data** but not do anything else with it.

The multi-academy trust must restrict the **processing** of **personal data**:

- Where it is in the process of considering a request for **personal data** to be rectified (see above);
- Where the multi-academy trust is in the process of considering an objection to processing by a **data subject**;
- Where the **processing** is unlawful but the **data subject** has asked the multi-academy trust not to delete the **personal data**; and
- Where the multi-academy trust no longer needs the **personal data** but the **data subject** has asked the multi-academy trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the multi-academy trust.

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

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

The Right to Be Forgotten

Data subjects have a right to have **personal data** about them held by the multi-academy trust erased only in the following circumstances:

- Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
- When a **data subject** withdraws consent – which will apply only where the multi-academy trust is relying on the individuals consent to the **processing** in the first place;
- When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
- Where the **processing** of the **personal data** is otherwise unlawful;
- When it is necessary to erase the **personal data** to comply with a legal obligation; and

The multi-academy trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

- To exercise the right of freedom of expression or information;
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, research or statistical purposes; or
- In relation to a legal claim.

If the multi-academy trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

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

The Right to Data Portability

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

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

16. Data security

We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**. For more information please refer to the Trust's **Network and IT Security Policy**.

We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.

Security procedures include, but are not limited to:

- **Entry controls.** Any unauthorised person seen in entry-controlled areas will be challenged and reported to the Headteacher.
- **Secure lockable desks and cupboards.** Desks and cupboards will be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required. IT assets will be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
- **Equipment.** Data users will ensure that individual monitors do not show confidential information to passers-by and that they either log off from their PC or lock the screen when it is left unattended.
- **Working away from the school premises – paper documents**. The only paper documents containing personal information which will be taken off the premises are; emergency contact details for residential trips, emergency contacts for holiday clubs, academy **Business Continuity Plans**. These will be kept securely by the **data user**.
- **Working away from the school premises – electronic working**. Only authorised devices will be permitted to be used for working offsite where the processing of personal data takes place. Appropriate safeguards will be put in place to ensure the security of data, as outlined in the Trust's **Network and IT Security Policy.**
- **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

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

17. Data Protection Impact Assessments

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

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

The Data Protection Impact Assessment will:

- Describe the nature, scope, context and purposes of the processing.
- Assess necessity, proportionality and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

When assessing levels of risk, the likelihood and the severity of any impact on individuals will be considered.

Future Generation Trust will complete an assessment of any such proposed **processing** and we have a template document which ensures that all relevant matters are considered.

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

18. Disclosure and sharing of personal information

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

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

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

19. Data processors

We contract with various organisations who provide services to Future Generation Trust, including, but not limited to:

- Connaught Communications Systems (CCTV)
- Scholarpack
- SchoolMoney (Eduspot)
- Parent App
- Entrust Education
- Edufin (Financial)
- Stoke City Council (Payroll)
- Haines Watts (Auditors)

- Teachers2Parents (Texts)
- Edit (Visitor Management)

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

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

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

20. Images and videos

Parents and others attending academy events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of an academy performance involving their child. Future Generation Trust does not prohibit this as a matter of policy.

Future Generation Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the multi-academy trust to prevent.

We ask that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

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

Whenever a pupil begins their attendance at the multi-academy trust they, or their parent/carer where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

21. CCTV

Future Generation Trust operates a CCTV system at some of our academy sites. Please refer to the Trust's **CCTV Policy**.

22. Biometric data

Future Generation Trust is committed to protecting the personal data of all its pupils and staff. This includes any biometric data that we may collect and process currently or in the future.

All biometric data will be collected and processed in accordance with relevant legislation and guidance to ensure the data and the rights of individuals are protected. For detailed information please refer to the Trust's **Protection of Biometric Information Policy**.

23. DBS data

All data provided by the Disclosure and Barring Service (DBS) will be handled in line with Data Protection Legislation; this includes electronic communication.

Data provided by the DBS will never be duplicated.

Any third parties who access DBS information will be made aware of this policy, as well as their responsibilities as a **data user**.

24. Cloud computing

For the purposes of this policy, **'**cloud computing**'** refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the trust accessing a shared pool of ICT services remotely via a private network or the internet.

All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the trust.

All files and personal data will be encrypted before they leave a trust device and are placed in the cloud, including when the data is 'in transit' between the device and cloud. A robust encryption key management arrangement will be put in place to maintain protection of the encrypted data. The loss of an encryption key will be reported to the DPO immediately; failure to do so could result in accidental access or destruction of personal data and, therefore, a breach of the relevant data protection legislation.

As with files on trust devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the trust should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the trust's policies for the use of cloud computing.

The trust's usage of cloud computing, including the service's security and efficiency, will be assessed and monitored by the DPO. The DPO will also ensure that a contract and data processing agreement are in place with the service provider, confirming compliance with the Data Protection legislation. The agreement will specify the circumstances in which the service provider may access the personal data it processes, such as the provision of support services.

The DPO will also:

- Ensure that the service provider has completed a comprehensive and effective self-certification checklist covering data protection in the cloud.
- Ensure that the service provider can delete all copies of personal data within a specified timescale.
- Confirm that the service provider will remove all copies of data, including back-ups, if requested.
- Find out what will happen to personal data should the trust decide to withdraw from the cloud service in the future.
- Assess the level of risk regarding network connectivity and make an informed decision as to whether the trust is prepared to accept that risk.
- Monitor the use of the trust's cloud service, with any suspicious or inappropriate behaviour of pupils, staff or parents being reported directly to the respective headteacher.

25. Monitoring and Review

Monitoring is the responsibility of the Future Generation Trust Board. Implementation and operational responsibility lies with the Headteacher at each academy.

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

This policy and all arrangements and procedures will be reviewed every two years.

Policy adopted on: **30 March 2023**

Review Date: **March 2025**

Signed: Fliss Dale **Designation:** Chair of Trust Board

Definition of Terms

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

Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by Future Generation Trust such as staff and those who volunteer in any capacity including Members, Trustees, Governors and parent helpers