DATA PROTECTION POLICY

FOR SCHOOLS WITHIN QUEST

St. Peter's C. of E. Primary School, Hindley
Hindley Green Community Primary School
St. John's C. of E. Primary School, Hindley Green
St. John's C. of E. Primary School, Abram
University Collegiate School, Bolton

September 2020
Review date September 2022

Data Protection Policy

1. Introduction

QUEST is committed to being transparent about what personal data is collected, how it is collected and the uses of the personal data of its pupils, their families, job applicants, potential employees, employees, contractors, agency staff, volunteers, apprentices and former employees, referred to as HR related personal data. The Data Protection Policy sets out the Trust's commitment to data protection, individual rights and obligations in relation to personal data.

The Trust may be required from time to time to share personal information about its employees, service users, pupils, or trainees with other organisations, mainly the LA, Department for Education, National College or other schools and educational bodies and potentially social services etc.

The Trust is the data controller (being the legal owner) of the data/information. The processors are our service providers such as LA, DfE, and SIMS Capita etc. as they have access to the data we own/control, and ensures the Trust complies with the core principles of the GDPR.

The Trust informs individuals the reasons for processing the individual's personal data, how it uses such data and the legal basis for processing it in its Privacy Notices. Personal data of individuals will not be processed for other reasons. The Trust will update all its personal data promptly if an individual advises that his/her information has changed or is inaccurate.

A copy of the Trust's Privacy Notices can be obtained from the DPO, Trust website or the GDPR software package – gdpr.co.uk

The Directors have appointed Janice Jones as the Data Protection Officer (DPO), Tonianne Hewitt as the Deputy DPO and the school's Admin officers as Data Guardians.

A Data protection officer (DPO) is appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- Work alongside Trust safeguarding leads to ensure that pupil/student data is protected as required.

2. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

This policy will also have regard to the Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)', Information Commissioner' Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now.

This policy will be implemented in conjunction with the following Trust policies:

- ICT, e-Safety and safer internet policy (plus Social networking advice and social medial policy).
- Freedom of Information Policy.
- Photographs and filmed images
- Disclosure Policy
- Safer Recruitment
- Safeguarding and Child protection

3. Scope

This policy applies to all personal data held by the schools and the Trust. It encompasses paper records; data held on computer and associated equipment, including CCTV, of whatever type and at whatever location, used by or on behalf of the Academy Trust.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The obligations outlined in this policy statement apply to all those who have access to personal data, whether employees, directors (or other public representatives), employees of associated organisations or volunteers. It includes those who work at home or from home, who must follow the same procedures as they would in an office environment.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. All individuals permitted to access personal data must agree to comply with this policy and failure to follow the policy may result in disciplinary procedures.

QUEST follows the data protection principals as set out below**:**

- The Trust processes personal data lawfully, fairly and in a transparent manner.
- The Trust collects personal data only for specified, explicit and legitimate purposes.
- The Trust processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Trust keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Trust keeps personal data only for the period necessary for processing.
- The Trust adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- Personal Data shall be processed in accordance with the right of data subjects under this Act.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with these principles".

3.1 Definitions of the different types of Data under the GDPR – Definitions taken from ICO
Personal Data - The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Special categories of personal data - Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

Special categories of personal data can include information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Criminal records data - means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Personal data is held in the individual's personnel file in hard copy and on the management information electronic system – including Wigan Council HR Systems (Payroll and HR Provider). The periods for which the Trust holds personal data are contained in appendix 2 – retention policy. Pupil data is held on the management information system and in hardcopy.

In accordance with the requirements of the General Data Protection Regulation (GDPR) the Trust keeps a record of all its processing activities in respect to personal data – further details available from DPO.

3.2 Individual rights
The GDPR provides the following rights for individuals:

3.2.1 The right to be informed
The Privacy Notice supplied to individuals in regards to the processing of their personal data is written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative, the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period and criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:
- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

If the data are used to communicate with the individual, at the latest, when the first communication takes place

3.2.2 The right of access
Individuals have the right to obtain confirmation that their data is being processed.
Individuals have the right to submit a subject access request (SAR) in writing to gain access to their personal data in order to verify the lawfulness of the processing.(See Section 8).

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within 1 month of receipt.

3.2.3 The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible.

Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, the Trust will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

3.2.4 The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information services to a child

The trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or
- statistical purposes
- The exercise or defense of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

3.2.5 The right to restrict processing

Individuals have the right to block or suppress the Trust's processing of personal data.
In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the

restriction is respected in future.

The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Trust has verified the accuracy of the data.
- Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual.
- Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- Where the trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Trust will inform individuals when a restriction on processing has been lifted.

3.2.6 The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a Contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The Trust will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

QUEST is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.

The Trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

3.2.7 The right to object

The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the Privacy Notices and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes, the Trust will stop processing personal data for direct marketing purposes as soon as an objection is received. The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes, the individual must have grounds relating to their particular situation in order to exercise their right to object.

Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

4. Collection of Data

The Academy Trust will inform data subjects of the reason why the data is being collected and to whom the data may be disclosed. See most recent Privacy Notices.

5. Consent

- Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.
- Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.
- Consent can be withdrawn by the individual at any time.
- The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

6. Accountability

QUEST will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The Trust will also provide comprehensive, clear and transparent Privacy Notices and ensure relevant and appropriate staff training. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

Internal records of processing activities will include the following:

- Name and details of the organisation.
- Purpose(s) of the processing.
- Description of the categories of individual's personal data.
- Retention schedules.
- Categories of recipients of personal data.
- Description of technical and organisational security measures.
- Details of transfers to third countries, including documentation of the transfer mechanism and safeguards in place.

The Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving its security features.

Data protection impact assessments will also be used, where appropriate.

7. Lawful processing

The legal basis for processing data will be identified and documented prior to data being processed. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official. Authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

7.1 Sensitive data will only be processed under the following conditions*:*

Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law. Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent. Processing relates to personal data manifestly made public by the data subject**.**

7.2 Processing

All processing of personal data will comply with the GDPR Principles. In the situation where data is processed by a third party, the third party will be required to act in a manner which ensures compliance with GDPR and they will be required to complete a data processor agreement between the Trust and the third party (appendix 1).

Data will only be processed for the purpose for which it was collected and should not be used for additional purposes without the consent of the data subject.

Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defense of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

8. Subject access requests

Individuals have the right to make a subject access request in writing and the Trust will verify the identity of the person making a request before any information is supplied. If an individual makes a subject access request, the Trust will tell him/her:

- Whether or not his/her data is processed and the reasons for processing/holding such data, the categories of personal data and how the data was sourced if it was not collected from the individual
- For how long his/her personal data is stored
- to whom his/her data is or may be disclosed, including to recipients located outside the European

Economic Area (EEA) and the safeguards that apply to such transfers
- His/her rights to correct or erasure of data, or to restrict or object to processing
- His/her right to complain to the Information Commissioner if he/she thinks the Trust has failed to comply with data protection rights
- Whether or not the Trust carries out automated decision-making and the logic involved in any such decision-making.

A copy of the information will be supplied to the individual free of charge; however, the trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format

The Trust will respond to a subject access request within 1 month of the date it is received. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

If a subject access request is manifestly unfounded or excessive, the Trust is not obliged to comply with it. Alternatively, the Trust can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

Where a request is manifestly unfounded or excessive, the Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify what information the request is in relation to.

10. Training

The Trust provides training to all individuals about their data protection responsibilities as part of the induction process.

11. Privacy by design and privacy impact assessments

The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to QUEST's reputation which might otherwise occur.

A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals, to determine the necessity and proportionality of processing.

A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:
- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

The trust will ensure that all DPIAs include the following information:
- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An outline of the risks to individuals

- The measures implemented in order to address and mitigate the risk.

Where a DPIA indicates high risk data processing, the trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

12. Data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The DPO will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

If the Trust discloses that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, the DPO will report it to the Information Commissioner with 72 hours of discovery. The Trust will record all data breaches regardless of their effect.

The risk of the breach having a detrimental effect on the individual, and the need to notify the Information Commissioner, will be assessed on a case-by-case basis.

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the DPO will inform the individual affected and inform them of the breach, provide information about likely consequences and the mitigation measures the Trust has taken.

In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitate decision-making in relation to whether the Information Commissioner, or the public need to be notified.

Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

13. International data transfers

The Trust will not routinely transfer HR-related or other personal data to countries outside the EEA.

If data is transferred outside the EEA on the basis of specific relevant safeguards e.g. declaration of adequacy, binding corporate rules or other safeguards, individuals would be consulted with prior to the Trust sharing any personal data with countries outside the EEA.

14. Data security

The Trust takes the security of personal data very seriously. The Trust has internal policies and controls in place to protect personal data against loss, accidental damage, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. e.g. systems restrictions and ICT data security policies.

Where the Trust engages third parties to process personal data on its behalf, (i.e. its payroll provider) such parties do so on the basis of written instructions, are under a duty of

confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

Confidential paper records will not be left unattended or in clear view anywhere with general access.

Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

Memory sticks will not be used to hold personal information and all electronic devices are password-protected to protect the information on the device in case of theft.

When leaving a computer unattended, staff must ensure they have either logged off their account or locked the computer to prevent anyone using their account in their absence.
Staff are not to share their username and password with other members of staff or anyone else.

Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.

Staff, directors and local advisory committee representatives will not use their personal laptops or computers for Trust purposes and will not download Trust documents onto personal laptop or computers.

All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

E-mails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

Circular emails to parents or a group of recipients are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

When sending confidential information by fax, staff will always check that the recipient is correct before sending.

Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Trust premises accepts full responsibility for the security of the data.

Before sharing data, all staff members will ensure:
- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a Privacy Notice.

Individuals may have access to the personal data of other individuals including those of our stakeholders in the course of their employment, contract, volunteer period or apprenticeship. Where this is the case, the Trust relies on individuals to help meet its data protection obligations to staff and to our stakeholders.

Individuals who have access to personal data are required:
- To access only data that they have authority to access and only for authorised purposes;
- Not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation.
- To keep data secure (for example by complying with rules on access to premises, computer access,

including password protection, and secure file storage and destruction).
- Not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device.
- Not to store personal data on local drives or on personal devices that are used for work purposes.

Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information are supervised at all times.
The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

QUEST takes its responsibilities under the GDPR seriously and any unauthorised disclosure or failing to observe these requirements may trigger a disciplinary offence, which will be dealt with under the Trust's Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing employee or stakeholder data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice

The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

15. CCTV and photography

The Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The Trust notifies all pupils, staff and visitors of the purpose for collecting CCTV images via the Privacy Notice

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

The Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

If the Trust wishes to use images/video footage of pupils in a publication, such as the Trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

16. Data retention

Data will not be kept for longer than is necessary, see appendix 2. Unrequired data will be deleted as soon as practicable.

Some educational records relating to former pupils or employees of the Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

17. DBS

All data provided by the 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 the data protection legislation, as well as their responsibilities as a data processor.

18. Monitoring

The Resources committee is responsible for auditing the data protection process and procedures.

This policy was revised during Autumn Term 2020 with due regard to the Equality Act 2010 and GDPR and approved by Directors on 8th September 2020 It will be reviewed every two years in line with the review cycle.

Signed: *B. Anthon* Chair of Board of Directors

APPENDIX

APPENDIX 1

DATA PROCESSOR AGREEMENT
BETWEEN QUEST AND XXXXXXX

Under the General Data Protection Regulation (GDPR). **QUEST** is required to put in place an agreement in writing with any organisation which processes personal data on its behalf to govern the processing of those data. This is to ensure anyone processing personal information on behalf of **QUEST** agrees to ensure the same level of security in respect of that information to ensure the Trust and its academies continue to meet their obligations under the GDPR.

Under a Service Level Agreement made between **QUEST** and **XXXXXXX** on 1st September 2019 ('the SLA") **Wigan Council** has agreed to provide a service to **QUEST** which requires **XXXXX** to have access to personal data for which **QUEST** is (and remains) the 'data controller' for the purposes of GDPR. The other party to this agreement, **XXXXX**, will be a 'data processor' under GDPR.

XXXXX agrees to store and process the personal data in accordance with the terms of this data processor agreement as set out below. The parties agree that the terms of this data processor agreement shall be incorporated and shall form part of the terms and conditions of the SLA. To the extent that any of the terms of this data processor agreement conflict with the terms of the SLA, the terms of this data processor agreement shall prevail.

1. Parties to the agreement:
QUEST and its schools **XXXXX** **Date of agreement 1st September 2019 to 31st August 2021**
2. Contacts
St. Peter's C. of E. Primary School, Hindley – 01942 258647 **Hindley Green Community Primary – 01942 255406** **St. John's C. of E. Primary, Hindley Green – 01942 255396** **St. John's C. of E. Primary, Abram – 01942 703465** **University Collegiate School, Bolton – 01204 928700**
3. Service to be provided
Provide a brief re. the service to be provided
4. Start and End date
This agreement is in line with the SLA for the above services commencing on 1st September 2019 and terminating on 31st August 2021. Should QUEST agree to extend the contract for the provision of the service with XXXXX beyond the SLA, this agreement will also need to be renewed.
5. Personal data to be provided to XXXXXX
Insert the type of personal data that will be processed.
6. Purposes for which the data are to be used

Insert the purpose for which the data is being processed.

7. Transmission of personal data

Data will be transferred via encrypted email, secure mailbox or encrypted file transfer

8. Security of personal data

*The data provided by **QUEST** must be loaded into the **XXXXX** Data Centre as soon as possible.*

***QUEST's** data must not be stored by **XXXXX** anywhere other than in the systems necessary to fulfil the SLA function.*

***QUEST's** data must never be transferred to Compact Disk, USB Stick, Laptop hard drives, External Hard Drive, paper or any other storage medium. Laptops must not be left unattended in unsecure locations including cars, hotel rooms or public areas. Laptops left unattended must be password locked at all times. All mobile devices must be encrypted.*

*Access to **QUEST's** data via **XXXXX** computer systems must be limited to those who have a business reason to know such information and are committed to confidentiality and secure process.*

XXXXX *must maintain firewalls to control access to its system and data, maintain an intrusion detection system to stop external threats and maintain incident response procedures specifically for occasions where intrusions do occur.* **XXXXX** *must have, and must provide **QUEST** with a copy of its plans and procedures for detecting and responding to any actual or attempted attack to gain unauthorised access to* **XXXXX** *systems. The above is covered in the Council's various IT security policies and we will work within these when providing services within the SLA.*

*All **QUEST** data must be maintained in encrypted form on servers that are behind* **XXXXX's** firewall*. All servers and all devices connecting to the* **XXXXX** *internal network must have the latest security patches, anti-virus software, firewalls installed in compliance with* **XXXXX's** *IT Policy – to be supplied as soon as possible.*

Access to **XXXXX's** *computer must require a combination of username and password. Passwords will be at least 7 characters long and consist of letters, numbers and symbols and will be changed in line with the Council's IT policy. Elevated user accounts and service accounts will require stronger passwords.*

XXXXX *must take reasonable and appropriate steps consistent with current technological developments to make sure that all **QUEST's** data and information is secure and to safeguard the integrity of records in storage and transmission.*

XXXXX *must:*

1.Take appropriate technical and organisational measures to protect against the unauthorised or unlawful processing of the personal data and against accidental loss or destruction of, or damage to, the personal data (including having adequate back-up procedures and disaster recovery systems) in order to comply with the seventh data protection principle;

2.Ensure that only employees who may be required to assist it in meeting its obligations under the Agreement shall have access to the personal data. **XXXXX** *shall ensure that all*

employees used by it to provide the services as described above and as defined in the Agreement have undergone training in the law of data protection and in the care and handling of personal data in light of the GDPR and have a valid enhanced DBS check/disclosure (where appropriate);

*3.Store the data it receives securely in line with **QUEST's** policies and destroy it securely as directed by the Academy Trust on the date the Agreement ends;*

4.Process the personal data only in accordance with the laws of the United Kingdom;

5.Not use the personal data for any purposes which are inconsistent with the purposes as described above and as defined in the Agreement;

*6.Not disclose the personal data to a third party in any circumstances other than at the specific request of **QUEST**;*

*7.In the event that any personal data in the possession or control of **XXXXX** becomes lost, corrupted or rendered unusable for any reason, **XXXXX** will promptly restore such personal data using its back up and/or disaster recovery procedures at no cost to **QUEST.***

*8.In the event that any personal data in the possession or control of **XXXXX** becomes lost, it will immediately inform **QUEST** with a full report as to the circumstances;*

*9. Not transfer any personal data outside the European Economic Area unless authorised to do so in writing by **QUEST.***

9. Retention of personal data

XXXXX will securely retain **QUEST's** data until completion or termination of the contract. On termination we will agree how the data is transferred back to **QUEST** or retained to assist with future queries.

10. Destruction of personal data

XXXXX will securely retain **QUEST's** data until completion or termination of the contract. On termination we will agree how the data is destroyed and the relevant destruction timescales.

11. Subject access requests

XXXXX has a process to manage Subject Access Requests and agrees to service where required, all subject access requests received seeking data held and managed by **XXXXX** under the SLA. Where these requests are received by **QUEST**, they will be sent to **XXXX to (email address).**

Any requests received in relation to information held by **XXXXX** that has derived from this agreement will be dealt with under this process and will be responded to within 1 month. However, **QUEST**, as the data controller, will approve and provide instructions relating to any responses.

12. Amending, transferring or deleting personal data

XXXXX must not amend any of **QUEST's** data without the prior consent of QUEST. **XXXXX** must not transfer any of **QUEST's** data to any external or third party for any reason. **XXXXX** must not delete any of **QUEST's** data other than at the end of the contract and in line with what is agree in the Destruction of Personal data section.

XXXXX will not engage another processor without prior written authorisation from the Trust/ school, where this is necessary to provide the functions of the SLA, the processor will also be bound by the same data protection terms as set out in this agreement.

13. Record-keeping and auditing compliance with this agreement

QUEST will store a copy of this agreement in the possession of the Chief Operating & Finance Officer. The COFO can at any time request and carry out a site visit to **XXXXX** to audit compliance to the agreement or the COFO may request such documents, or any other material, from **XXXXX** that will enable an audit of the agreement at any time.

14. Complaints

In the event of a complaint/allegation of misuse of personal information held by **XXXXX** on behalf of QUEST**,** the party who has received the complaint/allegation will immediately notify the other and, in co-operation with each other, they will follow the Council's process for managing data breaches and follow any advice from the Information Commissioner.

15. Breach of the data processor agreement

XXXXX agrees to assist the Trust/schools fulfil the requirements regarding the data rights of individual's (e.g access, delete or correct data) and data breaches concerning data processed on behalf of **QUEST** under the SLA. **QUEST** will inform its staff that XXXXX processes data on their behalf and provide them with a relevant privacy notice

XXXXX acknowledges and agrees that **QUEST** retain all rights, title and interest in the personal data subject to this agreement. **QUEST** remains the Data Controller and is responsible for the processing carried out by **XXXXX.**

Any indemnity to cover any monetary penalty, claim, loss, liability or costs incurred arising as a result of a breach of this Agreement by the Council or as a result of any negligence or breach of statute or common law in processing the information disclosed to it is provided as per the terms of the SLA.

16. Signatories

For QUEST:	**For XXXXXXXXXXX**:
Signed……	Signed……
Full name ……	Full name ……
……	……
Position……	Position……..
……	……
Date……	Date……

Appendix 2

QUEST
RETENTION OF RECORDS
IN LINE WITH GDPR

INTRODUCTION:
Management of Data is the process by which the Trust manages all aspects of any type of data in accordance with the General Data Protection Regulations (GDPR), whether internally or externally, from creation throughout their life cycle and to their eventual removal.

This data retention policy sets out the Trust's commitment to adhere to principal 5 of the GDPR, which states that Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

RELEVANT DATA PROTECTION PRINCIPLES:
The data protection principles which relate to the retention and removal of personal data are that personal data must:

- Be accurate and kept up to date (Principal 4).
- Not be kept longer than necessary for the purpose for which it was obtained (Principal 5).
- Be processed by a data controller who has in place appropriate technical and organisational measures to prevent unauthorised processing and accidental loss, destruction or damage.

RETENTION PERIODS:
In line with the fifth principle, QUEST will not retain Data any longer than necessary and in determining an appropriate retention period will take into account the following:

- The current and future value of the Data.
- The costs, risks and liabilities associated with retaining the Data.
- The ease or difficulty in ensuring the Data remains accurate and up-to-date.

APPROACH TAKEN WHEN MAKING A DECISIONS ABOUT RETAINING PERSONAL DATA?
QUEST believe it is good practice to regularly review the personal data held and delete anything that is no longer needed. Information that does not need to be accessed regularly, but which still needs to be retained, will be safely archived.

Standard retention periods for different categories of information will be established, taking into account any professional rules or regulatory requirements that apply.

The Trust will ensure that these retention periods are kept to in practice, by documenting and reviewing the retention policy. For example, if any records are not being used, it will be reconsidered, whether they need be retained.

ARCHIVES
Old accounting and personnel records, and some other records, will be archived until being disposed of. Archived records will be treated as being as confidential as current records.

RETENTION TIMESCALE:

1. Child Protection			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Child Protection files	Yes	DOB + 25 Years	Secure Disposal
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Secure Disposal

2. Directors			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Minutes			
• Principal set(signed)	No	Permanent	Retain in school for 6 years from date of meeting
• Inspection copies	No	Date of meeting + 3 years	Secure Disposal [If these minutes contain any sensitive personal information they should be shredded]
Agendas	No	Date of meeting	Secure Disposal
Reports	No	Date of meeting + 3 years	Retain in school for 6years from date of meeting.
Trusts and Endowments	No	Permanent	Retain in school whilst operationally required
Action Plans	No	Date of action plan + 3 years	Secure Disposal
Policy documents	No	Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)
Complaints files	Yes	Date of resolution of complaint + 6 years	Retaining school for the first six years Review for further retention in the case of contentious disputes Secure disposal routine complaints.
Annual Reports required by the Department for Education	No	Date of report+10years	
Proposals for schools to become, or be established as Specialist	No		Current year + 3 years

Status schools			

3. Management			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Minutes of the senior Management Team and other internal administrative bodies	Yes	Date of meeting + 5 years	Retain in the school for 5 years from meeting
Reports made by the head teacher or the management team	Yes	Date of report + 3 years	Retain in the school for 3 years from meeting
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes	Closure of file + 6 years	Secure Disposal
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No	Date of correspondence + 3 years	Secure Disposal
Professional development plans	Yes	Closure + 6 years	Secure Disposal
School development plans	Yes	Closure + 6 years	Review
Admissions -if the admission is successful	Yes	Admission + 1 year	Secure Disposal
Admissions - if the appeal is unsuccessful	Yes	Resolution of case + 1 year	Secure Disposal
Admissions - Secondary Schools -Casual	Yes	Resolution of case + 1 year	Secure Disposal
Proofs of address supplied by parents as part of the admissions process	Yes	Current year+1year	Secure Disposal
Supplementary Information form including additional information such as religion, medical conditions etc.	Yes	Admission year + 6years	Secure Disposal

4. Pupils			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Admission Registers	Yes	Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives
Attendance registers	Yes	Date of register+3 years	Secure Disposal [If these records are retained electronically any back-up copies should be destroyed at the same time]
Pupil files	Yes		
• Primary	Yes	Retain for the time which the pupil remains at the	Transfer to the secondary school (or

		primary school	other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit
• Secondary	Yes	DOB of the pupil + 25 years	Secure Disposal
Special Educational Needs files, reviews and Individual Education Plans	Yes	DOB of the pupil + 25 years the review, NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	Secure Disposal
Correspondence Relating to Authorised Absence and Issues	No	Date of absence + 2 years	Secure Disposal
Examination results	Yes		
• Public	No	Year of examinations + 6 years	Secure Disposal
• Internal examination results	Yes	Current year + 5 years if these records retained on the pupil file or in their National Record of Achievement they only be kept for as long as operationally necessary	Secure Disposal
Any other records created in the course of contact with pupils	Yes/No	Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or Secure Disposal
Statement maintained under The Education Act1996 - Section324	Yes	DOB + 30 years	Secure Disposal unless legal action is pending
Proposed statement or amended statement	Yes	DOB + 30 years	Secure Disposal unless legal action is pending
Advice and information to parents regarding educational needs	Yes	Closure + 12 years	Secure Disposal unless legal action is pending
Accessibility Strategy	Yes	Closure + 12 years	Secure Disposal unless legal action is pending
Parental permission slips for school trips - where there has been no major incident	Yes	Conclusion of the trip	Secure Disposal
Parental permission slips for school trips - where there has been a major incident	Yes	DOB of the pupil involved in the incident + 25 years	Secure Disposal

		The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	
Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	No	Date of visit + 14 years. This retention period has been set in agreement with the safeguarding children's officer.	N
Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	No	Date of visit + 10 years	N
Walking Bus registers	Yes	Date of register+3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	Secure Disposal [If these records are retained electronically any back-up copies should be destroyed at the same time

5. Curriculum			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
School Development Plan	No	Current year + 6years	Secure Disposal
Schemes of work	No	Current year+ 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or secure disposal
Timetable	No	Current year+ 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or secure disposal
Class record books	No	Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or secure disposal
Mark Books	No	Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or secure disposal
Record of homework set	No	Current year +1 year	It may be appropriate

			to review these records at the end of each year and allocate a new retention period or secure disposal
Pupils' work	No	Current year+1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or secure disposal
Examination results	Yes	Current year + 6 years	Secure Disposal
SATS records - Examination Papers and Results	Yes	Current year + 6 years	Secure Disposal
PAN reports	Yes	Current year + 6 years	Secure Disposal
Value Added & Contextual Data	Yes	Current year + 6 years	Secure Disposal
Self-Evaluation forms	Yes	Current year + 6 years	Secure Disposal

6. Personnel Records held in Schools			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Timesheets, sick pay	Yes	Current year + 6 years	Secure Disposal
Staff Personal files	Yes	Termination + 6 years	Secure Disposal
Interview notes and recruitment records	Yes	Date of interview + 6 months	Secure Disposal
Pre-employment vetting information (including DBS checks)	No	Date of check + 6 months	Secure Disposal
Disciplinary proceedings:	Yes	See below:	Secure Disposal [by the designated member of staff]
- Oral warning	Yes	Date of warning + 6 months	Secure Disposal
- Written warning-level one	Yes	Date of warning + 6 months	Secure Disposal
- Written warning -level two	Yes	Date of warning + 12 months	Secure Disposal
- final warning	Yes	Date of warning + 18 months	Secure Disposal
- case not found	Yes	If child protection related please child protection section. Otherwise secure disposal immediately at the conclusion of the case	Secure Disposal
Records relating to accident/injury at work	Yes	Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	Secure Disposal
Annual appraisal/assessment records	Yes	Current year + 6 years	Secure Disposal
Maternity pay records	Yes	Current year + 3 years	Secure Disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Current year + 6 years	Secure Disposal

Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes	Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff's personal file. Termination + 6 years	Secure Disposal

7. Health and Safety			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Accessibility Plans	No	Current year + 6 years	Secure Disposal
Accident Reporting			
• Adults	Yes	Date of incident + 7 years	Secure Disposal
• Children	Yes	DOB of child + 25 years. A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention this retention period has been applied.	Secure Disposal
COSHH	No	Current year+10 years [where appropriate an additional retention period may be allocated]	
Incident reports	Yes	Current year +20 years	Secure Disposal
Policy Statements	No	Date of expiry + 1 year	Secure Disposal
Risk Assessments	Yes	Current year+3 years	Secure Disposal
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	Yes	Last action + 40 years	Secure Disposal
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	Yes	Last action +50 years	Secure Disposal
Fire Precautions log books	No	Current year + 6 years	Secure Disposal

8. Administrative			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Employer's Liability certificate	No	Closure of the school +40 years	Secure Disposal
Inventories of equipment & furniture	No	Current year + 6 years	Secure Disposal
General file series	No	Current year + 5 years	Review to see whether a further

			retention period is required
School brochure or prospectus	No	Current year + 3 years	
Circulars (staff/parents/pupils)	No	Current year +1 year	Secure Disposal
Newsletters	No	Current year + 1 year	Review to see whether a further retention period is required
Visitors book	No	Current year + 2 years	Review to see whether a further retention period is required
PTA/Old Pupils Associations	No	Current year + 6 years	Review to see whether a further retention period is required
Emails	No	3 months	Deleted from system

9. Finance			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Annual Accounts	No	Current year + 6 years	
Loans and grants	No	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
Contracts			
• under seal	No	Contract completion date + 12 years	Secure Disposal
• under signature	No	Contract completion date + 6 years	Secure Disposal
• monitoring records	No	Current year+ 2 years	Secure Disposal
Copy orders	No	Current year + 2 years	Secure Disposal
Budget reports, budget Monitoring etc.	No	Current year+ 3 years	Secure Disposal
Invoice, receipts and other records covered by the Financial Regulations	No	Current year + 6 years	Secure Disposal
Annual Budget and background papers	No	Current year +6 years	Secure Disposal
Order books and requisitions	No	Current year+ 6 years	Secure Disposal
Delivery Documentation	No	Current year+ 6 years	Secure Disposal
Debtors' Records	No	Current year+ 6 years	Secure Disposal
Chequebooks	No	Current year+ 3 years	Secure Disposal
Paying in books	No	Current year + 6 years then review	Secure Disposal
Ledger	No	Current year + 6 years then review	Secure Disposal
Invoices	No	Current year+ 6 years then review	Secure Disposal
Receipts	No	Current year+ 6 years	Secure Disposal
Bank statements	No	Current year + 6 years then review	Secure Disposal
School Journey books	No	Current year + 6 years then review	Secure Disposal
Free school meals registers	Yes	Current year + 6 years	Secure Disposal
Petty cash books	No	Current year + 6 years	Secure Disposal

10. Property			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Title Deeds	No	Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
Plans	No	Permanent	Retain in school whilst operational
Maintenance and contractors	No	Current year + 6 years	Secure Disposal
Leases	No	Expiry of lease + 6 years	Secure Disposal
Lettings	No	Current year + 3 years	Secure Disposal
Burglary, theft and vandalism report forms	No	Current year + 6 years	Secure Disposal
Maintenance log books	No	Current year + 6 years	Secure Disposal
Contractors Reports	No	Current year + 6 years	Secure Disposal

11. Local Authority			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Secondary transfer sheets (Primary)	Yes	Current year + 2 years	Secure Disposal
Attendance returns	Yes	Current year +1 year	Secure Disposal

12. Department for Education			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
OFSTED reports and papers	No	Replace former report with any new inspection report	Review to see whether a further retention period is required
Returns	No	Current year + 6 years	Secure Disposal

13. Connexions			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Work Experience agreement	Yes	DOB of child + 18 years	Secure Disposal

14. Schools Meals			
Basic Files	Data Protection issue	Retention period	Action at the end of the administrative life of the record
Dinner Register	Yes	Current year + 3 years	Secure Disposal
School Meals Summary Sheets	No	Current year + 3 years	Secure Disposal