Data Protection Policy

Version Number	1.1
Date policy last reviewed	October 2023
Policy Type	Statutory
Owner	CEO
Approved By	The Trust Board
Approval Date	October 2023
Review Date	October 2024

Review Dates and Summary of Changes

Date	Summary of changes
February 2022	**Amended all references to GDPR to UK GDPR**
	Amended 2.1 to add it Name (including initials) Identification number Location data Online identifier, such as a username and Information on Special category Data
	5.6 removed named officer and telephone number
	17.4 removed reportable to Data Protection Office so member of senior management team will the contact
	Appendix 2 (point 3) removed phone number
	Appendix 7 – Point 3 changed Data Protection Act 1998 to Data Protection Act 2018
October 2022	Appendix 5- General Privacy Policy (a generic template policy) replaced with Privacy Notice for Staff
	Appendix 6- Employee Privacy Notice (a generic template policy) replaced with Privacy notice for students and parents
	Section added describing the role of Local Data Protection Leads, who will support the DPO
	References to DPO changed to include LDPL as required
	8.5 Removed as updating consents to match GDPR is complete
	8.6 replaced exception for preventative or counselling services with other legal basis
	18.4 'member of Senior Management Team' replaced with 'the LDPL'
	Personal Data Breach Procedure reports of breaches will be stored centrally, rather than on the headteacher's computer. Headteacher and DPO meeting replaces with LDPL and most appropriate leader.
	CCTV section removed and schools will now have specific CCTV and surveillance policies to reflect site specifics
	Data retention separated into its own policy

Signed by:

CEO Date: 10th October 2023

Chair of Trustees Date: 10th October 2023

Statement of Intent

The Omega Multi-Academy Trust ("the trust") is required to keep and process certain information about their staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (UK GDPR). The trust may, from time to time, be required to share personal information about their staff or pupils with other organisations, mainly the LA, Department for Education, other schools/trusts and educational bodies, children's services and other third parties, such as payroll providers or cashless till services.

This policy is in place to ensure all staff, governors and trustees are aware of their responsibilities and outlines how the trust comply with the following core principles of the UK GDPR. Organisational methods for keeping data secure are imperative, and the trust believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the UK GDPR, which came into effect on 25 May 2018.

1. Legal Framework

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

- The General Data Protection Regulation (UK 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

1.2 This policy operates in conjunction with the following Trust/school policies;

- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Online Safety Policy
- Photography and Images Policy
- Trust Financial Regulations
- Trust Record of Processing Activity
- Staff ICT and Electronic Devices Policy
- School Surveillance and CCTV Policy
- Trust Data Retention Policy

2. Applicable Data

2.1. For the purpose of this policy, **personal data** refers to any relating to an identified, or identifiable individual. This may include name (including initials), identification numbers, location data, online identifier (such as a user name or IP address). It may also include factors specific to the individuals physical, physiological, genetic, mental, economic, cultural or social identity. **Special Category Data** is personal data which is more sensitive and so needs more protection, including information about an individual's racial or ethnic origin, political opinions, religious of philosophical beliefs, trade union membership, genetics, biometrics (such as finger prints, retina and iris patterns) where used for identification purposes, health (physical or mental), sex life or sexual orientation.

2.2 The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.3. Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 2018. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. The UK GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

4. Accountability

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

4.2 The trust will provide comprehensive, clear and transparent privacy policies.

4.3. 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.

4.4. 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 individuals and personal data.
- Retention schedules.
- Categories of recipients of personal data.
- Description of technical and organisational security measures.
- Details of transfers to third countries where applicable, including documentation of the transfer mechanism safeguards in place.

4.5. 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 security features

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

5. Data Protection Officer (DPO)

5.1. A DPO will be appointed by the Trust central team in order to:

- Inform and advise the trust and its employees about their obligations to comply with the UK GDPR and other data protection laws.

- Monitor the trust's compliance with the UK 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.

5.2 An existing employee can be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests. Where possible, this role will be carried out by an external provider.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.4. The DPO will report to the highest level of management at the Trust, which is the CEO.

5.5.The DPO will operate independently and will not be dismissed or penalised for performing their task. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations. The Trust has appointed an external advisory service:

Head Office
The DPO Centre
50 Liverpool Street
London
EC2M 7PR

Regional Office
The DPO Centre
Suffolk Enterprise Centre
Felaw Street
Ipswich
IP2 8SQ

Our designated Data Protection can be contacted by email via dpo@omegamat.co.uk

6. Local Data protection Lead (LDPL)

6.1. A LDPL will be designated within each school and in the trust central team who will;

- Liaise with other LDPLs and the DPO to coordinate and deliver trust-wide data policy by;
    - Recording Subject access requests made to the school
    - Recording data breaches at the school
    - Performing due diligence and compliance to GDPR for new data processing
    - Inform and advise the school and its employees about their obligations to comply with the UK GDPR and other data protection laws

- Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments and organising the required training for staff members.

6.2. An existing employee can be appointed to the role of LDPL provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

6.3. The LDPL will report to the highest level of management at the school, which is the Headteacher.

7. Lawful Processing

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

- The consent of the data subject has been obtained.
- Processing is necessary for:
    - 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. (This condition is not available to processing undertaken by the trust in the performance of its tasks.)

7.2. 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.

7.3. 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 defence 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. Consent

8.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

8.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

8.3. Where consent is given, a record will be kept documenting how and when consent was given.

8.4 The trust ensures that consent mechanisms meet the standards of the UK 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.

8.5. Consent can be withdrawn by the individual at any time.

8.6. Where a child is under the age of 16 or younger if the law provides it (up to the age of 13), the consent of parents will be sought prior to the processing of their data, except where there is a legal basis for the processing of that data.

9. The Right to be Informed

9.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9.2. 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.

9.3. 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) and 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 if applicable and the safeguards in place.
- The retention period or 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.

9.4. 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, as well as any possible consequences of failing to provide the personal data, will be provided.

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

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

9.7. 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 is disclosed.
- If the data is used to communicate with the individual, at the latest, when the first communication takes place.

10. The Right of Access

10.1 Individuals have the right to obtain confirmation that their data is being processed.

10.2 Individuals have the right to submit a **Subject Access Request** (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

10.3. The trust will verify the identity of the person making the request before any information is supplied.

10.4. 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.

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

10.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.7. All fees will be based on the administrative cost of providing the information.

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

10.9. 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.

10.10. 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.

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

11. The Right to Rectification

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

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

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

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

11.5. 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.

12. The Right to Erasure

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

12.2. 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 society services to a child.

12.3. 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 defence of legal claims.

12.4. 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.

12.5. 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.

12.6. Where personal data has been made public within an online environment, the trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The Right to Restrict Processing

13.1. Individuals have the right to block or suppress the trust's processing of personal data.

13.2. 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.

13.3. 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.

13.4. 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.

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

14. The Right to Data Portability

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

14.2. 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.

14.3. 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.

14.4. Personal data will be provided in a structured, commonly used and machine-readable form.

14.5. The trust will provide the information free of charge.

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

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

14.8. 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.

14.9. The trust will respond to any requests for portability **within one month.**

14.10. 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.

14.11. Where no action is being taken in response to a request, the trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The Right to Object

15.1. 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 notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific or historical research and statistics.

15.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- 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.

15.4. 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.

15.5. 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.

15.6. Where the processing activity is outlined above, but is carried out online, the trust will offer a method for individuals to object online.

16. Automated Decision Making and Profiling

16.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2. The trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3. When automatically processing personal data for profiling purposes, the trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by Design and Privacy Impact Assessments

17.1. 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.

17.2. 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.

17.3. 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 the trust's reputation which might otherwise occur.

17.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5. A DPIA will be used for more than one project, where necessary.

17.6. 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 use of CCTV.

17.7. 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 risk.

17.8. 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.

18. Data Breaches

18.1. 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.

18.2. The Head Teacher of each school within the trust will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3. The Chief Executive will ensure all central service staff are made aware of, and understand what constitutes a data breach.

18.4. Staff must report any data breach or potential breach as soon as possible to the LDPL

18.5. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.6. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the trust becoming aware of it.

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

18.8. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the trust will notify those concerned directly.

18.9. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

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

18.11. 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 relevant supervisory authority or the public need to be notified.

18.12. 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.

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

18.14. In the unlikely event of a suspected Data breach, we will follow the procedure set out in Appendix 1.

19. Data Security

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

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

19.3. Digital data both on a local hard drive and on the trust's network is password-protected. The network drive is backed up daily off-site.

19.4. Access to the trust's network is controlled and access to sensitive and confidential data on the network is restricted to only those members of staff who require the information to perform their duties effectively.

19.5. Access to the trust's management information system SIMS is password-protected and access to sensitive and confidential data on SIMS is restricted to only those members of staff who require the information to perform their duties effectively.

19.6. As per the Staff ICT and Electronic Devices Policy, Staff are not permitted to use removable storage e.g. external hard drives or memory sticks to store data.

19.7. All electronic devices are password-protected to protect the information on the device in case of theft. Electronic devices are kept securely when not in use, e.g. in a locked cabinet.

19.8. All holding pupil and staff photos will be regularly wiped to delete all images. Memory cards will be kept in a locked cabinet when not in use and will be wiped regularly.

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

19.10. Staff, governors and student teachers, will not use their personal laptops or computers for school purposes.

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

19.12. Staff, governors and student teachers must not use personal email addresses for sharing or viewing any school data. Secure email accounts are provided for all staff and governors.

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

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

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

19.16. No personal data or sensitive personal data must be shared by text or on social media e.g. Whatsapp. See also the trust's e-Safety and IT Acceptable Use Policy.

19.17. 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 or paperwork under lock and key. The person taking the information from the trust premises accepts full responsibility for the security of the data.

19.18. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The person or organisation who will receive the data has been outlined in a privacy notice.
- The person or organisation who will receive the data have confirmed in writing that they comply with the GDPR and any other relevant data protection legislation.

19.19. Under no circumstances are volunteers, visitors or unauthorised third parties allowed access to confidential or personal information. Those visiting areas of the trust containing sensitive information are supervised at all times.

19.20. 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.

19.21. The trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.22. The Office Manager/Line Manager is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of Information

20.1. The trust has a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures.
- Minutes and meetings
- Financial information, such as Pupil Premium Grant or Sports Grant.

20.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

20.3. The trust schools will not publish any personal information, including photos, on its website without the permission of the individual.

20.4. When uploading information to the school/trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20.5. See individual schools for details of contact.

21. CCTV and Photography

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

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

21.3. Signage is placed visibly in areas where CCTV cameras are recording.

21.4. All CCTV footage will be kept for 30 days for security purposes; the Office Manager/Line Manager is responsible for keeping the records secure and allowing access.

21.5. The trust will always indicate its intentions for taking photographs of pupils and will obtain permission before publishing them.

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

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

22. Data Retention and Storing Pupil Data

22.1. Data will not be kept for longer than is necessary. The trust follows the Information Commissioner's guidance on retention of documents, including the

Information and Records Management Society's Retention Guidelines for School.

22.2. Unrequired data will be deleted as soon as practicable.

22.3. Some educational records relating to former pupils or employees of the trust may be kept for an extended period for legal reasons.

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

23. DBS Data

23.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2. Data provided by the DBS will never be duplicated.

23.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Monitoring and Review

24.1. This policy will be reviewed annually, ensuring that all procedures are up-to-date.

24.2. Any changes made to this policy will be communicated to all members of staff.

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO) found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Local Data Protection Lead (LDPL)

- The Local Data Protection Lead in conjunction with the DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidently or unlawfully:

    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The LDPL in conjunction with the DPO will alert the Chief Executive.

- The LDPL and DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The LDPL and DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

- The LDPL and DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, it will be considered whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal or pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the ICO must be notified.

- The LDPL will document the decision within school (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored centrally.

- Where the ICO must be notified, the LDPL will do this with support from the DPO via the 'report a breach page of the ICO website' found at https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- The LDPL will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

- The LDPL will document each breach, irrespective of whether it is reported to the ICO. For each breach, the record will include the:

    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of breaches will be stored centrally and will be periodically reported to Trustees.

- The LDPL and most appropriate leader (CEO, Head Teacher, Data Manager) will meet to discuss the severity of the breach and actions to mitigate risk and avoid future breaches, and refer to the DPO where appropriate.

Actions to minimise the impact of data breaches

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

Example of actions that would be taken in the event of a data breach:

- If special category data (is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the Local Data Protection Lead as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the Local Data Protection Lead will ask the ICT department to recall it

- In any cases where the recall is unsuccessful, the Local Data Protection Lead in conjunction with the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The LDPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

Appendix 2 – How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the department: https://www.gov.uk/contact-dfe