DATA PROTECTION POLICY

Adopted by the Trustees of
Leodis Academies Trust
4 July 2019

Document control table

Document title:	Data Protection Policy
Author:	DPO/Business Manager
Version number:	V3
Date approved:	
Approved by:	Trustees of Leodis Academies Trust
Date of review:	

Document History

Version	Date	Author	Note of revisions
V1	May 2018	DPO	
V2	Feb 2019	DPO/Business Manager	Addition of 'police' and 'health professionals and agencies including the NHS' that staff and student data may be shared with
V3	May 2019	DPO	Amendments to Subject Access Requests in Section 9

This policy applies to all members of Leodis Academies Trust (**Trust**). For the purposes of this policy, the term 'staff' means all members of staff within Leodis Academies Trust including permanent, fixed term and temporary staff. It also refers to governors, any third party representatives, agency workers and volunteers. All those who use or have access to the Trusts information must understand and adopt this policy and are responsible for ensuring the security of the information they use.

Leodis Academies Trust is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the EU's General Data Protection Regulation (**GDPR**).

The Trust may, from time to time, be required to share personal information about its staff or students with other organisations; mainly Local Authorities, other schools and educational bodies, other schools within the Leodis Academies Trust (including agencies via Leodis Support Service), police, health professionals and agencies including the NHS and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Trust complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are essential, and Leodis Academies Trust believes it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which will come into effect on 25 May 2018. The government have confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Leodis Academies Trust is the Data Controller (**Controller**) and will determine the purposes for which, and the manner in which, any personal data are, or are to be, processed. The Trustees will have overall responsibility for compliance with the GDPR.

The Trustees have delegated responsibility to the Principal in each Academy for ensuring compliance with the GDPR and this policy within the day-to-day activities of their Academy.

Distribution
East Ardsley Primary Academy
Hill Top Primary Academy
Westerton Primary Academy
Woodkirk Academy

CONTENTS PAGE

1. LEGAL FRAMEWORK

1.1. This policy has due regard to legislation, including, but not limited to:

1.1.1. The General Data Protection Regulation.

1.1.2. The Freedom of Information Act 2000.

1.1.3. The Education (Student Information) (England) Regulations 2005 (as amended in 2016).

1.1.4. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

1.1.5. The School Standards and Framework Act 1998.

1.2. This policy also has regard to the guidance:

ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'.

1.3. This policy must be implemented in conjunction with the following Trust/Academy policies:

1.3.1. Freedom of Information.

1.3.2. IT Usage.

1.3.3. CCTV (unless managed by PFI provider).

2. APPLICABLE DATA

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, for example an IP address. The 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, for example key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. 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 GDPR, personal data must be:

3.1.1. Processed lawfully, fairly and in a transparent manner in relation to individuals.

3.1.2. 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.

3.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.1.4. 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.

3.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods, insofar as the personal data must 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 GDPR in order to safeguard the rights and freedoms of individuals.

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

4. ACCOUNTABILITY

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

4.2. The Trust must provide comprehensive, clear and transparent privacy policies.

4.3. Additional internal records of the Trust's processing activities must include the following

4.3.1. Name and details of the organisation.

4.3.2. Purpose(s) of the processing.

4.3.3. Description of the categories of individuals and personal data.

4.3.4. Retention schedules.

4.3.5. Categories of recipients of personal data.

4.3.6. Description of technical and organisational security measures.

4.3.7. Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

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

4.4.1. Data minimisation.

4.4.2. Pseudonymisation.

4.4.3. Transparency.

4.4.4. Allowing individuals to monitor processing.

4.4.5. Continuously creating and improving security features.

4.5. Data protection impact assessments must be used, where appropriate.

5. DATA PROTECTION OFFICER

5.1. A Data Protection Officer (DPO) will be appointed in order to:

5.1.1. Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.

5.1.2. 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.

5.2. If the DPO is an existing employee the Trust will ensure that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3. The individual appointed as DPO must 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, which is the **Executive Board**.

5.5. The DPO will operate independently.

5.6. Agreed resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. LAWFUL PROCESSING

6.1. The legal basis for processing data must be identified and documented prior to data being processed.

6.2. Under the GDPR, data must be lawfully processed under the following conditions:

6.2.1. The consent of the data subject has been obtained.

6.2.2. Processing is necessary for:

6.2.2.1. Compliance with a legal obligation.
6.2.2.2. The performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.
6.2.2.3. For the performance of a contract with the data subject or to take steps to enter into a contract.
6.2.2.4. Protecting the vital interests of a data subject or another person.
6.2.2.5. 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.)

6.3. Sensitive data must only be processed under the following conditions:

6.3.1. Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.

6.3.2. 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.

6.3.3. Processing relates to personal data manifestly made public by the data subject.

6.3.4. Processing is necessary for:

6.3.4.1. Carrying out obligations under employment, social security or social protection law, or a collective agreement.
6.3.4.2. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
6.3.4.3. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
6.3.4.4. 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.
6.3.4.5. 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.
6.3.4.6. 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.
6.3.4.7. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

7. CONSENT

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

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

7.3. Where consent is given, a record must be kept documenting how and when consent was given.

7.4. The DPO must ensure 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.

7.5. Consent accepted under the Data Protection Act 1998 will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under this Act will not be reobtained.

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

7.7. Where a student is under the age of 16, the consent of parents must be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a student.

8. THE RIGHT TO BE INFORMED

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

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

8.3. In relation to data obtained both directly and indirectly from the data subject, the following information will be supplied within the privacy notice:

8.3.1. The identity and contact details of the Controller (and where applicable, the Controller's representative) and the DPO.

8.3.2. The purpose of, and the legal basis for, processing the data.

8.3.3. The legitimate interests of the Controller or third party.

8.3.4. Any recipient or categories of recipients of the personal data.

8.3.5. Details of transfers to third countries and the safeguards in place.

8.3.6. The retention period of criteria used to determine the retention period.

8.3.7. The existence of the data subject's rights, including the right to:

8.3.7.1. Withdraw consent at any time
8.3.7.2. Lodge a complaint with the Information Commissioner's Office.

8.3.8. The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

8.4. 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, must be provided.

8.5. 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, must be provided.

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

8.7. In relation to data that is not obtained directly from the data subject, this information must be supplied:

8.7.1. Within one month of having obtained the data.

8.7.2. If disclosure to another recipient is envisaged, at the latest, before the data is disclosed.

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

9. THE RIGHT OF ACCESS

9.1. Individuals have a right to make a "Subject Access Request" to gain access to personal information that the Trust holds about them. This includes:

9.1.1. Confirmation that their personal data is being processed.

9.1.2. Access to a copy of the data.

9.1.3. The purposes of the data processing.

9.1.4. The categories of personal data concerned.

9.1.5. Who the data has been, or will be, shared with.

9.1.6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

9.1.7. The source of the data, if not the individual

9.1.8. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

9.2. Subject access requests should be submitted in writing, either by letter or email to the Principal at their Academy.

9.3. They should include:

9.3.1. Name of individual

9.3.2. Correspondence address

9.3.3. Contact number and email address

9.3.4. Details of the information requested

9.4. If a member of staff receives a subject access request they must immediately notify the Principal at their Academy.

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

9.6. Students below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers may be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.7. Students aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.8. When responding to requests, we:

9.8.1. May ask the individual to provide two forms of identification

9.8.2. May contact the individual via phone to confirm the request was made

9.8.3. Will respond without delay and within one month of receipt of the request

9.8.4. Will provide the information free of charge

9.8.5. May tell the individual we will comply within three calendar months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

9.9. We will not disclose information if it:

9.9.1. Might cause serious harm to the physical or mental health of the student or another individual

9.9.2. Would reveal that the student is at risk of abuse, where the disclosure of that information would not be in the student's best interests

9.9.3. Is contained in adoption or parental order records

9.9.4. Is given to a court in proceedings concerning the student

9.10. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

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

9.12. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10. THE RIGHT TO RECTIFICATION

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

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

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

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

10.5. 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 Information Commissioner's Office and to a judicial remedy.

11. THE RIGHT TO ERASURE

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

11.2. Individuals have the right to erasure in the following circumstances:

11.2.1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.

11.2.2. When the individual withdraws their consent.

11.2.3. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

11.2.4. The personal data was unlawfully processed.

11.2.5. The personal data is required to be erased in order to comply with a legal obligation.

11.2.6. The personal data is processed in relation to the offer of information society services to a student.

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

11.3.1. To exercise the right of freedom of expression and information.

11.3.2. To comply with a legal obligation for the performance of a public interest task or exercise of official authority.

11.3.3. For public health purposes in the public interest.

11.3.4. For archiving purposes in the public interest, scientific research, historical research or statistical purposes.

11.3.5. The exercise or defence of legal claims

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

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

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

12. THE RIGHT TO RESTRICT PROCESSING

12.1. Individuals have the right to block or suppress the Trust's processing of personal data in line with legal and statutory guidelines.

12.2. In the event that processing is restricted, the Trust must 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 respect in future.

12.3. The Trust must restrict the processing of personal data in the following circumstances:

12.3.1. Where an individual contests the accuracy of the personal data, processing must be restricted until the Trust has verified the accuracy of the data.

12.3.2. Where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual.

12.3.3. Where processing is unlawful and the individual opposes erasure and requests restriction instead.

12.3.4. Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

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

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

13. THE RIGHT TO DATA PORTABILITY

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

13.2. 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.

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

13.3.1. To personal data that an individual has provided to a controller.

13.3.2. Where the processing is based on the individual's consent or for the performance of a contract.

13.3.3. When processing is carried out by automated means.

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

13.5. The Trust must provide the information free of charge.

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

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

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

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

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

13.11. Where no action is being taken in response to a request, the Trust must, without delay and at the latest within one month, explain to the individual the reason for this and must inform them of their right to complain to the Information Commissioner's Office and to a judicial remedy.

14. THE RIGHT TO OBJECT

14.1. The Trust must inform individuals of their right to object at the first point of communication, and this information must 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.

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

14.2.1. Processing based on legitimate interests or the performance of a task in the public interest.

14.2.2. Direct marketing.

14.2.3. Processing for purposes of scientific or historical research and statistics.

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

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

14.3.2. The Trust must 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.

14.4. Where personal data is processed for direct marketing purposes:

14.4.1. The Trust must stop processing personal data for direct marketing purposes as soon as an objection is received.

14.4.2. The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

14.5.1. The individual must have grounds relating to their particular situation in order to exercise their right to object

14.5.2. 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.

14.6. Where the processing activity is outlined above, but is carried out online, the Trust must offer a method for individuals to object online.

15. AUTOMATED DECISION MAKING AND PROFILING

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

15.1.1. It is based on automated processing, for example profiling.

15.1.2. It produces a legal effect or a similarly significant effect on the individual.

15.2. The Trust must 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.

15.3. When automatically processing personal data for profiling purposes, the Trust must ensure that the appropriate safeguards are in place, including:

15.3.1. Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

15.3.2. Using appropriate mathematical or statistical procedures.

15.3.3. Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

15.3.4. Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

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

15.4.1. The Trust has the explicit consent of the individual.

15.4.2. The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

16. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

16.1. The Trust must 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.

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

16.3. 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.

16.4. A DPIA must 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.

16.5. A DPIA must be used for more than one project, where necessary.

16.6. High risk processing includes, but is not limited to, the following:

16.6.1. Systematic and extensive processing activities, such as profiling.

16.6.2. Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

16.6.3. The use of CCTV.

16.7. The Trust must ensure that all DPIAs include the following information:

16.7.1. A description of the processing operations and the purposes.

16.7.2. An assessment of the necessity and proportionality of the processing in relation to the purpose.

16.7.3. An outline of the risks to individuals.

16.7.4. The measures implemented in order to address risk.

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

17. DATA BREACHES

17.1. 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.

17.2. The Principal must ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

17.3. All breaches must be reported to the DPO.

17.4. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commissioner's Office must be informed.

17.5. All notifiable breaches must be reported to the Information Commissioner's Office within 72 hours of the Trust becoming aware of it.

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

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

17.8. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the Information Commissioner's Office.

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

17.10. 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's Office or the public need to be notified.

17.11. Within a breach notification, the following information must be outlined:

17.11.1. The nature of the personal data breach, including the categories and approximate number of individuals and records concerned.

17.11.2. The name and contact details of the DPO.

17.11.3. An explanation of the likely consequences of the personal data breach.

17.11.4. A description of the proposed measures to be taken to deal with the personal data breach.

17.11.5. Where appropriate, a description of the measures taken to mitigate any possible adverse effects.

17.12. 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. DATA SECURITY

18.1. Staff must adhere to the IT Usage Policy.

18.2. Confidential paper records must be kept in a locked filing cabinet, drawer or safe, with restricted access. Any records relating to child protection must be kept in a locked cabinet in a locked room.

18.3. When printing or photocopying personal data it must be collected immediately in person and not left on the tray.

18.4. Confidential paper records must not be left unattended or in clear view anywhere with general access. This includes boxes of confidential waste not yet destroyed.

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

18.6. Staff who have access to a radio (walkie talkie) must keep messages to a minimum and be discreet. No personal information should be given when using the device.

18.7. Noticeboards displaying personal data relating to students must not be in an area accessible or visible to visitors or students.

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

18.9. Memory sticks must not be used to hold personal information unless they are password-protected and fully encrypted.

18.10. All electronic devices must be password-protected (and encrypted) to protect the information on the device in case of theft.

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

18.12. Staff and Governors must not use their email addresses, personal laptops or computers as a long term store for Trust personal data relating to staff or students. Data must only be downloaded/stored for temporary use and deleted as soon as the task has been completed.

18.13. Trust email accounts must not be used to register for or store personal data on third party online systems without IT staff/Third Party IT Provider checking that appropriate security and privacy notices have been provided for the system by the company.

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

18.15. Passwords must not be shared with other users and must be unique, ie not the same ones used for other systems.

18.16. Email must only be used as a last resort for sharing personal details. Other secure solutions should be sought first. If email is still required, any containing sensitive or confidential information must be password-protected or encrypted.

18.17. All devices must be logged-out or locked when unattended or not in use.

18.18. Circular emails to parents (for example, e-newsletter) or emails sent to multiple parents must be sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.19. When sending confidential information by post, fax, email or any other method, staff must always check that the recipient address/contact number is correct before sending.

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

18.21. Before sharing data, all staff members must ensure:

18.21.1. They are allowed to share it.

18.21.2. That adequate security is in place to protect it.

18.21.3. Who must receive the data has been outlined in a privacy notice.

18.22. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust containing sensitive information must be supervised at all times.

18.23. The physical security of the Trust's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage must be put in place.

18.24. The Leodis Academies Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.25. All Third Party systems and providers who use personal data about staff or students in the Trust must be checked to ensure privacy policies are up to date and that their systems are secure.

18.26. The Leodis Academies Trust must not publish any personal information, including photos, on its website without the permission of the affected individual.

19. CCTV AND PHOTOGRAPHY

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

19.2. The Trust notifies all students, staff and visitors of the purpose for collecting CCTV images via signage and privacy notices.

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

19.4. The Trust must always indicate its intentions for taking photographs of students and must retrieve permission before publishing them.

19.5. If the Trust wishes to use images/video footage of students in a publication, such as the Trust's website or Academy website/prospectus, permission must be sought for the particular usage from the parent of the student.

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

19.7. Monitors are in a secure location and are not on view to students, members of staff, parents or visitors per se. Only persons approved by the Principal or members of the Senior Leadership Team can access the CCTV area and those staff must be inducted into using the room and their responsibilities with regard to CCTV images as appropriate. All discs and recording equipment are kept in a secure location where access is strictly controlled.

19.8. Access to images by Trust staff is restricted to staff who need to have access in order to achieve the purpose(s) of using the equipment (as designated by the Principal, or senior members of the Pastoral team).

19.9. Further information is available in the Academy's CCTV policy.

20. DATA RETENTION

20.1. Data must not be kept for longer than is necessary and in accordance with the IRMS guidance Information Management Toolkit for Schools.

20.2. Data which is no longer needed must be deleted as soon as practicable.

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

20.4. Paper documents must be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data no longer needs to be retained.

21. STAFF RESPONSIBILITIES

21.1. It is important that all members of Leodis Academies Trust understand what is required of them and comply with this policy. This policy does not form part of the formal contract of employment for staff but it is a condition of employment that employees abide by the rules and policies made by Leodis Academies Trust from time to time. Any breach of this policy will be taken seriously and may result in disciplinary action.

21.2. Any member of staff who considers that the policy has not been followed in respect of their personal data should raise the matter with their Principal.

21.3. All staff are responsible for checking that any information they provide in connection with their employment is accurate and up to date and should inform their Academy of any changes, for example change of address. Leodis Academies Trust cannot be held responsible for any errors unless the member of staff has advised them of such changes.