GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

DOCUMENT CONTROL

Author/Contact	Stephen Lester Tel: 01946 820356 Email: contactus@westlakesmat.org.uk	
Document Path & Filename	Staff General/Corporate Information/Policies and Procedures/General/General Data Protection Regulation (GDPR) Policy	
Document Reference	General Data Protection Regulation (GDPR) Policy	
Version	01 West Lakes MAT	
Status	Approved	
Publication Date	29th October 2018	
Related Policies		
Review Date	October 2019	
Approved/Ratified by	Board of Trustees	29th October 2019

Distribution:

West Lakes Multi-Academy Trust Employees

Please note that the version of this document contained within the Policy Folder on Staff General is the only version that is maintained.

Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Version	Date	Comments	Author
05 WLA		WLA policy	S Lester
01 MAT		Updated April 2019 to take account of required additional reporting procedures.	S Lester

GENERAL DATA PROTECTION POLICY

Contents:

1. STATEMENT OF INTENT

1.1 West Lakes Multi Academy Trust (WLMAT, the Trust) is committed to protecting the rights and privacy of individuals in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 The Trust is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the General Data Protection Regulation (GDPR) for various purposes such as:

- To support student learning;
- To monitor and report on student progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To ensure we operate efficiently and effectively;
- To recruit and pay staff;
- To collect money;
- To comply with legal obligations to funding bodies and the government;
- To enable financial modelling and planning;
- To develop a comprehensive picture of the workforce and how it is deployed.

1.3 The Trust may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the Department for Education, Cumbria County Council, other schools and educational bodies and social services.

1.4 This policy is in place to ensure all staff, members, trustees and governors are aware of their responsibilities and outlines how the trust complies with the principles of the GDPR.

1.5 This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage, audio and video systems.

1.6 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 GDPR, which came 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.

2. LEGAL FRAMEWORK

2.1. 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 (Student 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

2.2. This policy also has regard to the following guidance:

Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'

Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3. ASSOCIATED POLICIES

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

- Photographic Consent
- ICT, Social Media & Internet Use Policy
- Freedom of Information Policy
- CCTV Policy

4. DEFINITIONS

4.1 **'Personal data'** refers to any information that relates to an identifiable, living individual (**'data subject'**). This includes information such as names, addresses, telephone numbers, photographs, expressions of opinion about an individual, or an online identifier (for example an IP address or roll number). 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, e.g. key-coded.

4.2 **'Special categories of personal data'** refers to information which is broadly the same as 'sensitive personal data' previously referred to in the Data Protection Act (DPA) 1998. This includes biometric data, ethnicity, religious beliefs, data concerning health matters and actual or alleged criminal activities.

4.3 **'Processing' refers** to any operation which is performed on personal data such as: collection, recording, organisation, storage, alteration, retrieval, use, disclosure,

dissemination or otherwise making available, combination, restriction, erasure or destruction.

4.4 **'Data Controller' refers** to any individual or organisation who controls personal data, in this instance West Lakes Multi Academy Trust.

4.5 **'Data Subject'** refers to an individual who is the subject of the personal data, for example:

- Employees (current and former),
- Students (including former students),
- Recruitment applicants (successful and unsuccessful),
- Agency workers (current and former),
- Casual workers (current and former),
- Contract workers (current and former),
- Volunteers (including members, trustees, directors and governors) and those on work placements

5. COMPLIANCE

5.1 Compliance with this policy is the responsibility of all the members of West Lakes MAT who process or have access to personal data (including trustees and governors).

5.2 Any breach of this policy will result in disciplinary procedures being invoked. A serious or deliberate breach could lead to dismissal.

5.3 Personal information will only be shared where it is lawful to do so and the third party agrees to abide by this policy and complies with the principles of the GDPR.

5.4 This policy will be updated, as necessary, to reflect best practice in data management, security and control and to ensure compliance with any change or amendment to the GDPR and any other relevant legislation.

6. PRINCIPLES

6.1. In accordance with the requirements outlined in the GDPR (Article 5), personal data will be:

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

6.3. 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.

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

6.5. Accurate and, where necessary, kept up-to-date; ensuring that inaccurate personal data is erased or rectified without delay.

6.6. 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 GDPR in order to safeguard the rights and freedoms of individuals.

6.7. 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.

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

6.9. The trust will only process personal data in accordance with individuals' rights and will comply with article 5 of the GDPR in the following ways:

6.10. By making all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purpose of the processing; any disclosures to third parties that are envisaged; an indication of the period for which the data will be kept, and any other information which may be relevant.

6.11. By ensuring that the reason for which the personal data was originally collected is the only reason for which it is processed, unless the individual is informed of any additional processing before it takes place.

6.12. By not seeking to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

6.13. By reviewing and updating personal data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate. Individuals must notify WLA if a change in circumstances means that their data needs to be updated. It is the responsibility of WLA to ensure that any notification regarding a change is acted on swiftly. WLA may also contact individuals to verify certain items of data.

6.14. By undertaking not to retain personal data for longer than is necessary to ensure compliance with the legislation, any other statutory requirements and the Records Management policy. This means WLA will undertake a regular review of the information held.

6.15. By disposing of any personal data in a way that protects the rights and privacy of the individual concerned

6.16. By ensuring appropriate technical and organisational measures are in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data

6.17. Personal data may be stored for longer periods and may be processed solely for archiving in the public interest, scientific or historical research, or statistical purposes.

7. ACCOUNTABILITY

7.1. West Lakes Multi Academy Trust is the registered Data Controller with the Information Commissioner's Office (ICO) and is responsible for controlling the use and processing the personal data it has collected.

7.2. The Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR. This includes:

7.3. Providing comprehensive, clear and transparent privacy notices (Appendix 1 and 2).

7.4. Using data protection impact assessments (DPIA), where appropriate (Appendix 3).

7.5. Recording activities relating to higher risk processing, such as the processing of special categories of personal data

7.6. The privacy notices (Appendices 1 and 2) explain how the Trust will share personal data with third parties. The Data Protection Officer will ensure that sharing only takes place when consent has been given. The sharing of personal data is generally limited to enabling the Trust to perform its statutory duties or in respect to a student's health, safety and welfare.

7.7. Records of activities relating to higher risk processing will be maintained as required, such as the processing of special categories data or that in relation to criminal convictions and offences.

7.8. 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, including documentation of the transfer mechanism safeguards in place

7.9. Individuals who provide personal data to the Trust are responsible for ensuring that the information provided is accurate and up-to-date.

7.10. 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.

7.11. Data Protection Impact Assessments will be used, where appropriate.

8. DATA PROTECTION OFFICER (DPO)

8.1. The DPO appointed by West Lakes Multi Academy Trust is Maureen McKendry, Business Manager at St Bernard's Catholic High School Barrow-in Furness.

They will:

Ensure staff, trustees and governors are informed about their obligations to comply with the GDPR and other data protection laws including recognising a subject access request, data security and off-site use.

Ensure staff, trustees and governors are aware of and understand what constitutes a data breach.

Ensure annual training is provided on the contents of this policy and develop and encourage best practice in all Trust Academies.

Ensure there is liaison with any external data controllers engaged with the Trust.

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 ensuring the required training to staff members.

Ensure continuity and recovery methods are in place to ensure the security of personal data.

Ensure obsolete personal data is properly erased and a destruction log is maintained. This will include the document description, classification, date of destruction, method and authorisation.

Be the point of contact with the ICO, cooperate with any requests and ensure that the Trust's notification is kept accurate.

Maintain up to date knowledge of data protection law in relation to schools.

Ensure confidentiality in relation to their role and any findings as a result of their role.

8.2. The DPO reports to the Trust's Chief Executive Officer

8.3. The DPO will operate independently and will not be dismissed or penalised for performing their task.

8.4. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

9. LAWFUL PROCESSING

9.1. The legal basis for processing data will be identified and documented prior to data being processed.

9.2. Under the GDPR, data will be lawfully processed under the following conditions:

9.3. Consent of the data subject has been obtained

9.4. Processing is necessary for:

9.5. Compliance with a legal obligation

9.6. Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

9.7. Performance of a contract with the data subject or to take steps to enter into a contract.

9.8. Protecting the vital interests of a data subject or another person.

9.9. 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.

9.10. Sensitive data will only be processed under the following conditions:

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

9.12. 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.

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

9.14. Processing is necessary for:

9.15. Carrying out obligations under employment, social security or social protection law, or a collective agreement

9.16. Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

9.17. The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

9.18. Reasons of substantial public interest on the basis of European Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.

9.19. 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.

9.20. Reasons of public interest in the area of public health.

9.21. Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9.22. Safeguarding students.

9.23. The Trust collects and uses workforce information for general purposes under paragraphs 9.2.2.2 and 9.3.4.4 of this policy which complies with Articles 6 and 9 of the GDPR. Under any other circumstances the legal basis for processing data will be identified and documented prior to data being processed.

10. CONSENT

10.1. It is not always necessary to obtain consent, see sections 9.2 and 9.3, but when it is, consent must always be a positive indication.

10.2. Consent must be a positive indication; it cannot be inferred from silence, inactivity or pre-ticked boxes.

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

10.4. Any forms used to gather personal data will be provided with a privacy notice (Appendices 1 and 2) and will indicate whether or not the individual needs to give consent for the processing. Records will be kept documenting how and when consent was given.

10.5. The Trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, and there is no other lawful basis on which to process the data then the Trust will ensure that the processing of that data does not take place.

10.6. 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.

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

10.8. 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.

11. THE RIGHT TO BE INFORMED

11.1. Privacy notices regarding the processing of personal data (obtained either directly or indirectly) will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

11.2. 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.

11.3. 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 data controller and the DPO.

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

The legitimate interests of the data controller or third party.

Any recipient or categories of recipients to whom the personal data will be disclosed.

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

The retention period of 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.

11.4. 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 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 at the time of collection.

11.5. 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.

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

11.7. 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 are disclosed.

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

12. THE RIGHT OF ACCESS

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

12.2. 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. In order to ensure that individuals receive the correct information SARs must be made in writing using the Trust SAR form and submitted to the CEO of the Trust (Appendix 4)

12.3. The Trust will verify the identity of the person making the request before any information is supplied.

12.4. 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.

12.5. Where a fair processing request is made the information contained within the relevant privacy notice will be provided.

12.6. Where a SAR is made, copies of personal data will generally be encrypted and supplied to the individual in a commonly used electronic format.

12.7. Where a SAR is received from a student the Trust's policy is that:

12.8. It will be processed in the same way as any other SAR. The information will be given directly to the student, unless it is clear that the student does not understand the nature of the request.

12.9. Where a student does not appear to understand the nature of the request it will be referred to their parents or carers.

12.10. A SAR from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the information will be sent either in a sealed envelope or electronically to the requesting parent(s). This will be provided within 15 academy days in accordance with the current Education (Pupil Information) Regulations.

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

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

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

12.14. 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.

12.15. 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.

12.16. 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 is in relation to.

13. THE RIGHT TO RECTIFICATION

13.1. Personal data held by the Trust will be as accurate as reasonably possible.

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

13.3. Where an individual informs the Trust of inaccurate or incomplete personal data their data record will be updated as soon as it is practicable.

13.4. A printout of a student's personal data record held on the Trust's information management systems will be provided to parents / carers every twelve months so they can check its accuracy and make any amendments.

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

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

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

13.8. 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.

14. THE RIGHT TO ERASURE

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

14.2. 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

Where the personal data was unlawfully processed

Where the personal data is required to be erased in order to comply with a legal obligation

Where the personal data is processed in relation to an online service

14.3. 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 establishment, exercise or defence of legal claims

14.4. 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.

14.5. 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.

14.6. Where personal data has been made public within an online environment and is then requested to be erased, taking account of the available technologies and the costs of implementation, all reasonable steps will be taken to inform other organisations who process the personal data to erase links to and copies of the personal data in question.

15. THE RIGHT TO RESTRICT PROCESSING

15.1. Individuals have the right to block or suppress the Trust's processing of personal data.

15.2. 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.

15.3. 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

15.4. 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.

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

16. THE RIGHT TO DATA PORTABILITY

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

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

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

To personal data that an individual has provided to the Trust

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

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

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

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

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

16.8. 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.

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

16.10. 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.

16.11. 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.

17. THE RIGHT TO OBJECT

17.1. The Trust will inform individuals of their right to object at the first point of communication; this information will be outlined in the privacy notice (Appendices 1 and 2).

17.2. 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.

17.3. 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.

17.4. 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.

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

18. PRIVACY BY DESIGN AND PRIVACY IMPACT ASSESSMENTS

18.1. When new data system, processing or software changes are being proposed ('a project') 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.

18.2. 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. (Appendix 3).

18.3. DPIAs will allow the Trust to identify and resolve problems at an early stage, thus preventing reputational damage which might otherwise occur.

18.4. 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.

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

18.6. 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

18.7. 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

18.8. 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.

19. DATA BREACHES

19.1. 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.

19.2. The Chief Executive Officer 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.

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

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

19.5. 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.

19.6. 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.

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

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

19.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust, which facilitates decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

19.10. 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

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

20. DATA SECURITY

20.1. The Trust undertakes to ensure the security of personal data it has collected. Personal data will only be accessible to those who have a valid reason for using it.

20.2. All staff, trustees and governors of the trust are responsible for ensuring that any personal data they hold is kept secure and not disclosed to any unauthorised third party (a data security user checklist is provided for quick reference in Appendix 5).

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

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

20.5. 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.

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

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

20.8. All electronic devices (computers, tablets, laptops, mobile phones) are password-protected, with a strong password, to protect the information on the device in case of theft.

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

20.10. When Staff, Trustees and Governors use their personal laptops or computers for trust purposes involving personal data they must ensure that all equipment is secure, files are encrypted and no other person can access any personal data on the laptop or computer.

20.11. Password rules are in place. All members of staff who require computer and network access are provided with their own secure login and password, and the system is set to require users to regularly and routinely change their passwords.

20.12. Unique user names and passwords for separate systems and software are required as detailed in the ICT, Social Media and Internet Use Policy.

20.13. Emails containing attachments with sensitive or confidential information are password-protected.

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

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

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

20.17. Before sharing data, all staff, trustees and governors 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

20.18. Physical security measures include:

20.19. Premises security measures such as access controls, visitor management, alarms, safes, deadlocks.

20.20. Only authorised personnel are allowed in the Network Support Office

20.21. Disks, tapes, printouts are locked away securely when not in use.

20.22. 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.

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

20.24. Technical measures include:

20.25. security software on all Trust networks and electronic devices,

20.26. internet filtering and firewalls,

20.27. anti-virus software,

20.28. ransomware detection.

20.29. Users are assigned a clearance that will determine which files and folders are accessible to them. Confidential and protected files are not accessible to unauthorised users.

20.30. Memory storage devices (such as USB memory sticks and removable hard drives) can only be used to hold personal data under the following conditions: the device must be checked by a Network Support Technician before use; it must be password protected or encrypted; it must be stored in a secure place when not in use; it must not be used or accessed by other users, including family members; personal data must be securely deleted when no longer required.

20.31. Organisational measures include:

20.32. Paper records containing personal data must not be left unattended or in clear view anywhere with general access

20.33. Paper records and removable storage devices must be stored in a secure and safe place.

20.34. Paper records containing personal data must be kept secure if they are taken off the Trust's premises.

20.35. Staff must sign the Trust's Acceptable Use Policy before being given access to the Trust's computers or network.

20.36. Passwords must be 'strong'

20.37. User names and passwords must not be shared.

20.38. All devices that are used to access personal data (including computers, tablets, laptops and mobile phones) must be locked even if left unattended for short periods.

20.39. Computers and CCTV monitors that show personal data must be placed so that they are not visible except to authorised staff.

20.40. Circular emails must be sent blind carbon copy (bcc) so that they do not disclose other recipients email addresses.

20.41. Visitors must not be allowed to see personal data unless they have a legal right to do so or previous consent has been given.

20.42. Visitors to areas of Trust premises containing special categories of personal data must be supervised at all times.

20.43. Personal data must not be given over the telephone unless absolutely sure of the identity of the person you are speaking to and they have the legal right to request it.

20.44. Personal data must not be disclosed to any unauthorised third parties.

20.45. Personal electronic devices must not be used to hold personal data belonging to the Trust.

20.46. Personal electronic devices must be password protected and have up to date active anti-virus and malware checking software before being used to access personal data belonging to the Trust.

20.47. Personal electronic devices that have been set to automatically log in to the Trust's network, email accounts or Google drives that have been lost or stolen must be reported to the COO so that access to the systems can be reset.

20.48. Personal data must not be stored as local copies on personal electronic devices

20.49. Personal data may only be taken off site if there is a specific business need.

20.50. If personal data is taken off site in electronic or paper form, extra care must be taken to follow strict security procedures. The person taking the personal data must accept full responsibility for the security of the data.

20.51. Before sharing personal data staff, trustees and governors must ensure: they are allowed to share it; that adequate security is in place to protect it; who will receive the personal data has been outlined in a privacy notice.

20.52. Staff, trustees and governors are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

20.53. West Lakes Multi Academy Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

20.54. The Chief Operating Officer is responsible for ensuring business continuity and recovery measures are in place to ensure the security of protected data.

20.55. Data breach detection tests will be undertaken to evaluate the Trust's technical measures and minimise the chance of a data breach.

21. PUBLICATION OF INFORMATION

21.1. West Lakes Multi Academy Trust publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

Policies and procedures

Annual reports

Financial information

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

21.3. West Lakes Multi Academy Trust will not publish any personal information, including photos, video and audio, on its website without the permission of the individual.

21.4. When uploading information to the Trust or individual academy website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

22. CCTV, VIDEO, AUDIO AND PHOTOGRAPHY

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

22.2. The Trust notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

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

22.4. All CCTV footage will be kept for six months for security purposes; the Data Protection Officer is responsible for keeping the records secure and allowing access.

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

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

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

23. DATA RETENTION

23.1. Data will not be kept for longer than is necessary.

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

23.3. Some educational records relating to former students 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.

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

24. DATA DISPOSAL

25. The Trust will comply with the requirements for safe destruction and deletion of data when it is no longer required.

26. Paper documents containing personal data will be shredded or disposed of as confidential waste and appropriate contract terms will be put in place with any third parties undertaking this work.

27. Hard drives of redundant PCs and storage devices containing personal data will be securely wipes clean before disposal, or if that is not possible, physically destroyed.

28. A Destruction Log will be retained of all personal data that is disposed of. This will include the document description, classification, date of destruction, method and authorisation.

29. DBS DATA

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

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

29.3. 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.

30. SECURE TRANSFER OF DATA

26.1 The Trust is required to share personal information with the Department for Education (DfE), Education and Skills Funding Agency (ESFA), Cumbria County Council (CCC), Ofsted, schools and educational institutions, public services and other third party providers. These are outlined in the privacy notices (Appendix 1 and 2).

26.2 Trust users must not remove, copy or share any personal data with a third party without permission from the DPO.

26.3 Where personal data is required to be lawfully shared with a third party it must be securely transferred either through a portal or be sent following encryption, using approved encryption software, and be password protected.

31. TRAINING AND AWARENESS

31.1. All Trust users receive GDPR training on an annual basis. They are made aware of their responsibilities as described in this policy through: induction training for new staff; staff meetings/briefings/INSET; day to day support and guidance

32. POLICY REVIEW

32.1. This policy is reviewed every two years by the Chief Operating Officer, Data Protection Officer and the Chief Executive Officer.

The next scheduled review date for this policy is January 2021.

Appendix 1

Privacy Notice: How we use Student Information in West Lakes Multi Academy Trust

The categories of student information that we collect, process, hold and share include:

- Personal information (such as name, contact details and unique student number);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctors' information, child health, dental health, allergies, medication, dietary requirements and notes from meetings/GPs/other health care professionals)
- Attendance information (such as sessions attended, number of absences and absence reasons and any previous schools attended).
- Assessment and attainment information (such as Key Stage results, reports, feedback, test data, exam results post 16 courses enrolled for and any relevant results)
- Special Educational Needs information (such as Education and Health Care Plans (EHCPs), Individual Education Plans (IEPs) and notes from review meetings and professional assessments)
- Behavioural information such as exclusions and any relevant alternative provision put in place) and behaviour information
- Information on trips and visits, catering, free school meals management, identity management and authentication

Post 16 learning information and destination data

Why we collect and use this information

We use the student data for the following purposes:

- To support student learning;
- To monitor and report on student attainment progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To comply with the law regarding data sharing;
- To keep children safe (food allergies or emergency contact details)
- To meet statutory duties placed upon us for DfE data collections

The lawful basis on which we use this information

We collect and use student information for general purposes under paragraphs 9.2.2.2 and 9.3.4.4 of the trust GDPR policy which complies with Articles 6 and 9 of the GDPR.

In addition concerning any special category data:

- Conditions which comply with Article 9 of the GDPR.

How we collect student information

We collect student information via registration forms at joining the Trust and refresh information (including by electronic means) throughout the time at the Trust and via Common

Transfer File (CTF) or secure file transfer from previous schools, local authorities and/or Department for Education (DfE).

Student data is essential for the Trust's operational use. Whilst the majority of student information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain student information to us or if you have a choice in this.

How we store student data

We hold student data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please see our data retention schedule.

Who we share student information with

We routinely share student information with:

- schools that students attend after leaving us;
- Cumbria County Council;
- The Department for Education (DfE);
- Other public services that have a lawful right to collect student information;
- Youth support services (students aged 13+)
- Third parties as listed in Appendix 6 of the GDPR policy.

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

Why we share student information

We share student information with the DfE on a statutory basis. This information sharing underpins school funding and educational attainment policy and monitoring. We are required to share information about our students with the DfE under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

Data collection requirements

To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to:
https://www.gov.uk/education/data-collection-and-censuses-for-schools

Youth support services
Students aged 13+

Once our students reach the age of 13 we will also pass student information to Inspira as they have responsibilities in relation to the education of 13-19 year olds under section 507B of the Education Act 1996 and The Education and Schools Act 2008. This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / student once he/she reaches the age 16.

Data is securely transferred to the youth support service via the DfE on a statutory basis and are stored and held for as stated in our Records Management Policy.

A parent or guardian can request that **only** their child's name, address and date of birth is passed on to Inspira by informing the Academy Leadership Group PA or other designated person at individual academies. This right is transferred to the student once they are 16.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services (Inspira) as they have responsibilities in relation to the education of 13-19 year olds under section 507B of the Education Act 1996 and The Education and Schools Act 2008. This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services;
- careers advisers.

For more information about services for young people, please visit Cumbria County Council's website:
www.cumbria.gov.uk/

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections.

We are required to share information about our students with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.
For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to their personal information. To make a request for your personal information, or be given access to your child's educational record, contact the Academy Leadership Group's PA or the designated person at each academy.

You also have the right to:

- object to processing of personal information that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to redress either through the ICO or through the courts.

If you have a concern or complaint about the way we are collecting or using your personal information, we request that you raise your concern with us in the first instance or directly to the Information Commissioner's Office at: https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice please contact:

Maureen McKendry
Data Protection Officer
West Lakes Multi Academy Trust
Main Street
Egremont
Cumbria
CA22 2DQ

How Government uses your data

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

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- Informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Student Progress measures).
- Supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data Collection requirements

To find out more about the data collection requirements placed on use by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about students in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police, please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Appendix 2

Privacy Notice: How we use Staff School Workforce Information (including other Adults*) in West Lakes Multi Academy Trust

***other adults include volunteers, governors, trustees and members**

The categories of workforce information that we collect, process, hold and share include:

- Personal information (such as name, employee or teacher number, national insurance number);
- Special categories of data including characteristics information (such as gender, age, ethnic group);
- Contract information (such as start dates, hours worked, post, roles and salary information);
- Work absence information (such as number of absences and reasons);
- Qualifications and, where relevant, subjects taught;
- Relevant medical or disability information (such as access arrangements, medication and occupational health reports);
- Payroll information (such as address, age, gender, bank account details);
- Pension details.

Why we collect and use this information

We use workforce data to:

- Ensure we can operate efficiently and effectively;
- Enable individuals to be paid;
- Allow for better financial modelling and planning;
- Enable the development of a comprehensive picture of the workforce and how it is deployed;
- Inform the development of recruitment and retention policies.

The lawful basis on which we process this information

We collect and use workforce information for general purposes under paragraphs 9.2.2.2 and 9.3.4.4 of this policy which complies with Articles 6 and 9 of the GDPR.

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain workforce information to us or if you have a choice in this.

Storing workforce information

The length of time we hold workforce information is set out in our Records Management policy.

Who we share this information with

We routinely share this information with:

- Cumbria County Council
- the Department for Education (DfE)
- other schools or organisations following reference requests
- other public services that have a lawful right to collect workforce information
- Payroll provider
- third parties listed in Appendix 6 of the GDPR policy.

Why we share workforce information

We do not share workforce information with anyone without consent unless the law and our policies allow us to do so.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment. We are required to share information about our workforce with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Academy Trusts) and local authorities that work in state funded schools. All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements including the data that we share with the DfE go to: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE 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 DfE 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 workforce information, organisations must comply with the DfE's terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of data.

For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the DfE go to:
https://www.gov.uk/contact-dfe

Requesting access to our personal data

Under data protection legislation, you have the right to request access to your information. To make a request for your personal information, contact Karen Wond, HR Officer.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we collect or use your personal data, we ask that you raise your concern with Karen Wond, HR Officer, in the first instance. Alternatively, you can contact the Information Commissioner's Office at: https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact:
Maureen McKendry, Data Protection Officer:
West Lakes Multi Academy Trust
Main Street
Egremont
Cumbria
CA22 2DQ

Appendix 3
Data Protection Impact Assessment (DPIA) Process

1. Overview

- A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.
- We must do a DPIA for certain listed types of processing, or any other processing that is **likely to result in a high risk** to individuals' interests. We use a screening checklist (developed by the Information Commissioners Office) to help decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- The DPIA must:
- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.
- To assess the level of risk, we consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- We will consult the Academy DPO and, where appropriate, individuals and relevant experts. Processors may need to assist.
- If we identify a high risk and we cannot mitigate that risk, we must consult the ICO before starting the processing.
- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. In appropriate cases we may issue a formal warning not to process the data, or ban the processing altogether.

2. Checklists

2.1 DPIA awareness checklist:

- We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- Our existing policies, processes and procedures include references to DPIA requirements.
- We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA where necessary.
- We have created and documented a DPIA process.
- We provide training for relevant staff on how to carry out a DPIA.

2.2 DPIA screening checklist

We always carry out a DPIA if we plan to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

We consider carrying out a DPIA if we plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic monitoring.
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.

If we decide not to carry out a DPIA, we document our reasons.

We consider carrying out a DPIA in any major project involving the use of personal data.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

2.3 DPIA process checklist

- We describe the nature, scope, context and purposes of the processing.
- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- We ask for the advice of our data protection officer.
- We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

- We identify measures we can put in place to eliminate or reduce high risks.
- We record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- We implement the measures identified, and integrate them into our project plan.
- We consult the ICO before processing if we cannot mitigate high risks.
- We keep our DPIAs under review and revisit them if necessary.

3. In brief

What is new under the GDPR?

The GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If our DPIA identifies a high risk which we cannot mitigate, we must consult the ICO.

This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

DPIAs are now mandatory in some cases, and there are specific requirements for content and process.

We will embed the DPIA process into our organisational policies and procedures.

In the run-up to 25 May 2018, we also need to review your existing processing operations and decide whether we need to do a DPIA for anything which is likely to be high risk. We will not need to do a DPIA if we have already considered the relevant risks and safeguards, unless there has been a significant change to the nature, scope, context or purposes of the processing.

4. What is a DPIA?

A DPIA is a process to systematically analyse our processing and help to identify and minimise data protection risks. It must:

- describe the processing and purposes;
- assess necessity and proportionality;
- identify and assess risks to individuals; and
- identify any measures to mitigate those risks and protect the data.

It does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified.

We must do a DPIA for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability more generally and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It is important to embed DPIAs into organisational processes and ensure the outcome can influence our plans. A DPIA is not a one-off exercise and should be seen as an ongoing process, kept under regular review.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – whether physical, material or non-material - to individuals or to society at large.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context and purposes of the processing.

5. When do we need to do a DPIA?

We must do a DPIA before you begin any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals.

5.1 In particular, the GDPR says we must do a DPIA if we plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

5.2 The ICO also requires us to do a DPIA if we plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

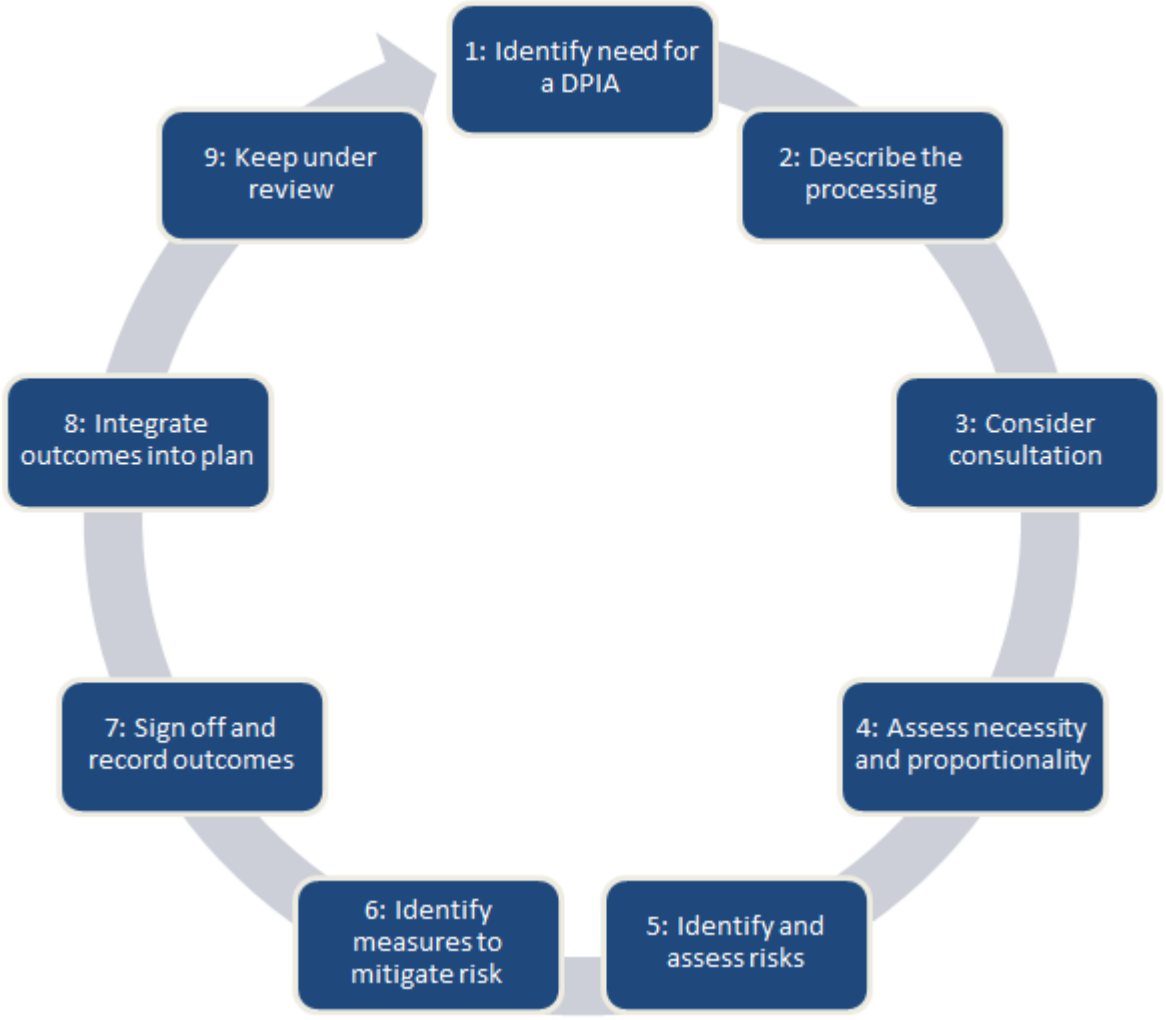
5.3 We should also think carefully about doing a DPIA for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

5.4 Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

6. How do we carry out a DPIA?

6.1 A DPIA should begin early in the life of a project, before we start our processing, and run alongside the planning and development process. The process to be used is attached in Appendix 1.

6.2 It includes these steps:



6.3 We must seek the advice of our data protection officer. We should also consult with individuals and other stakeholders throughout this process.

6.4 The process is designed to be flexible and scalable

6.5 DPIAs will be published, with sensitive details removed if necessary.

7. Do we need to consult the ICO?

7.1 If we have carried out a DPIA that identifies a high risk, and we cannot take any measures to reduce this risk, we need to consult the ICO. We cannot go ahead with the processing until we have done so.

The focus is on the ‘residual risk’ after any mitigating measures have been taken. If our DPIA identified a high risk, but we have taken measures to reduce this risk so that it is no longer a high risk, we do not need to consult the ICO.

We need to complete the ICO online form and submit a copy of our DPIA.

Once the ICO has the information they need, they will generally respond within eight weeks (although they can extend this by a further six weeks in complex cases).

The ICO will provide a written response advising us whether the risks are acceptable, or whether we need to take further action. In some cases the ICO may advise not to carry out the processing because they consider it would be in breach of the GDPR. In appropriate cases the ICO may issue a formal warning or take action to ban the processing altogether.

References

Information Commissioners Office (retrieved April 2018)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

WEST LAKES MULTI ACADEMY TRUST

DATA PROTECTION IMPACT ASSESSMENT (DPIA) PROCESS

Title of new system or change to existing system

33. 1. Identify the need for a DPIA

Does the proposed new system or change in existing system require a DPIA? Use the DPIA checklist is section 2.2. If yes, continue. If no, record the basis for this decision.

34. 2. Describe the processing

2.1 Describe the nature, scope, context and purposes of the processing.

35. 3. Consider consultation

3.1 Note which data processors need to be contacted to help understand and document their processing activities and identify any associated risks.

3.2 Consider how best to consult individuals (or their representatives) and other relevant stakeholders. Summarise your conclusions.

3.3 Contact our data protection officer and ask for advice. Summarise their advice.

4 Assess necessity and proportionality

4.1 Check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.

5 Identify and assess risks

5.1 Do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

6 Identify measures to mitigate risks

6.1 Identify measures we can put in place to eliminate or reduce high risks.

7 Sign off and record outcomes

7.1 Record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

8 Integrate outcomes into plan

8.1 Note the measures identified. State how these will be implemented and integrate them into the project plan.

8.2 Consult the ICO before processing if we cannot mitigate high risks. Note the details of the consultation including dates and responses.

9 Keep under review

DPIAs must be kept under review and revisited if necessary. Note date for review.

Name:

Signed:

Date:

Appendix 4

SUBJECT ACCESS REQUEST
ACCESS TO PERSONAL
DATA REQUEST

Enquirer's Forenames	
Enquirer's Surname	
Enquirer's Address	
Enquirer's Postcode	
Enquirer's Tel No	

	Yes/No
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?	
Do you have the parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? **If Yes:**	
Name of child or children about whose personal data records you are enquiring	

Description of Concerns/Area of Concern

Description of information or Topic(s) Requested (In your own words)

Additional Information

Please despatch Reply to: (if different from enquirer’s details as stated on this form)

Name

Address

Postcode

DATA SUBJECT
DECLARATION

I request that West Lakes Multi Academy Trust searches its records based on the information supplied above under the GDPR and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the Trust.

I agree that the reply period will commence when I have supplied sufficient information to enable the
Trust to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

_____

Name of "Data Subject" (or Subject's Parent) (PRINTED)

Dated _____

Appendix 5

WEST LAKES MULTI ACADEMY TRUST DATA SECURITY USER CHECKLIST

This checklist applies to all West Lakes Multi Academy Trust staff, Members, Trustees and Governors and refers to personal data belonging to West Lakes Multi Academy Trust (as the data controller):

- Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.
- Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject/project folders and worksheets can be stored in classrooms).
- Paper records containing personal data **must** be kept secure if they are taken off the trust premises.
- Trust users **must** sign an acceptable user policy (AUP) prior to being given access to the trust network. This will be up-dated periodically.
- Passwords **must** be alphanumeric, including one capital and one special character, and be a minimum of 8 characters long to access the trust network and Google Drive.
- Trust user names and passwords **must not** be shared.
- Trust electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.
- Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.
- Emails **must** be encrypted if they contain personal data and are being sent outside the EU.
- Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
- Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
- Visitors to trust premises containing special categories of personal data **must** be supervised at all times.
- Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.
- Personal data **must not** be disclosed to any unauthorised third parties.
- Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:

    - The device **must** be checked by a Network Support Technician before use;
    - It **must** be password protected;

- It **must** be stored in a secure and safe place when not in use;
- It **must not** be accessed by other users (e.g. family members) when out of a Trust Academy.

- Personal data **must** be securely deleted (in accordance with the Trust's policies) when no longer required.

- Personal electronic devices **must not** be used to hold personal data belonging to the Trust.

- Personal electronic devices **must** be password protected and have up-to-date, active anti-virus and anti-malware checking software before being used to access personal data belonging to the Trust via:

  - A password protected removable storage device;
  - The remote desktop protocol (i.e. remote access to the trust network);
  - Google Drive (including Google docs, Google classroom etc.).

- Personal electronic devices that have been set to automatically log into the trust network, trust email accounts or Google drive that are lost or stolen **must** be reported immediately to the DPO so that access to these systems can be reset.

- Google file download can be used but copies of documents containing personal data **must not** be stored as local copies on the personal electronic device.

- If personal data is taken off Trust premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the trust premises **must** accept full responsibility for data security.

- Before sharing personal data, Trust staff / Members / Trustees / Governors **must** ensure:

  - They are allowed to share it;
  - That adequate security is in place to protect it;
  - Who will receive the personal data has been outlined in a privacy notice.

- Any personal data archived on disks **must** be kept securely in a lockable cabinet.

- Trust staff are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

Appendix 6

THIRD PARTY SUPPLIERS WITH ACCESS TO
WEST LAKES MULTI ACADEMY TRUST
PERSONAL DATA

A2C
Academy ICT Services
Access
Activelearn
ALPS
BCS
Barnados
Bedrock
Biostore
Burnetts Solicitors – HR Advisors
CCTV
CPU
CPOMS
Capita SIMS
Caterlink / CRB Cunningham (Cashless Catering) [Including Biometric Data]
Choose Occupational Health
Civica
Companies House
Compucover
Cumbria County Council School Admissions
Cumbria County Council Children's Services
Cumbria County Council School Transport Team
Cycleshare
Department for Education (various sites and sections)
Doodle
Dr Frost maths
Educare
Edulink
EDX
EEF Smart Spaces Science
Exam Boards: AQA, BCS, Pearson, Edexel, OCR, Eduqas,
FFT Aspire
Facebook
Freedomtech
Future Learn
G4S
Gen2
Google
Google Smart Cloud
Group Call
Group Call on demand
Hegarty Maths
Helen Hinvest
Inspira
Instagram
IRIS

JTRS
Kerboodle
Khan Academy
Kym Allan
Lakes College (Apprenticeships)
Learner Records Service (LRS)
Lightspeed MDM
Local Government Pension Scheme
MCC
MicroLibrarian
Microsoft (Office suite, Office 365 and Outlook email)
Milk
Mint class
NCA Tools
NCTL
O2
Onscreen Platform (POP)
Open Study College
Parents Evening Booking System
ParentMail
Paxton
Pearl Scanning Group
Pinpoint Learning
PiXL apps
Pearson Activeteach
Room Booking System (remove 1 April 2019)
SIMS (including SIMS Activities)
SISRA online
Sage payroll
School Asset Manager
School ICT Services
School Nurse Services
School iP (Derventio Education)
Seneca
Sodhexo (Childcare vouchers)
Staff Absence Management Ltd
Storyboardthat
Survey Monkey
Tassimi
Teachers' Pension Scheme
Telephone system
Tempest Photography
Times Tables Rock Stars
Twitter
UCAS
UKCRB
Unifrog
University of Cumbria
University of Durham
Westfield Health
Work Experience Companies (various)

Note that where usernames are required for computer and network access West Lakes Multi Academy Trust use, students Network Usernames rather than their actual names.

Appendix 7

WEST LAKES MULTI ACADEMY TRUST

LETTER TO THIRD PARTY SUPPLIERS / DATA PROCESSORS TO CONFIRM COMPLIANCE WITH GDPR

Dear

West Lakes Multi Academy Trust has been required to comply with the General Data Protection Regulation (GDPR) since 25th May 2018.

As a third-party supplier / data processor we need you to confirm that you have undertaken a review of your processes and procedures to comply with the GDPR.

Please complete the series of questions below and explain how you will comply (the text is taken directly from the GDPR).

28(3) Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller.

The contract must stipulate, in particular, that the processor will:

Requirement	Confirm consent and process
28(3)(a) process only on documented instructions, including regarding international transfers (unless, subject to certain restrictions, legally required to transfer to a third country or international organisation); 28(3)(b) ensure those processing personal data are under a confidentiality obligation (contractual or statutory)	
28(3)(c) take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate.	

28(3)(d) only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors; 28(3)(e) assist the controller in responding to requests from individuals (data subjects) exercising their rights.	
28(3)(f) assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36).	
28(3)(g) delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law).	
28(3)(h) make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.	

Organisation name	
Address	
Name of authorised person	
Position	
Signature of authorised person	

Please complete this form and return it to Stephen Lester, Chief Operating Officer lesters@westlakesacademy.org.uk