THE TRUE LEARNING PARTNERSHIP
GDPR Data Protection Policy

April 2019

Contents:

Statement of intent

The TRUE Learning Partnership is required to keep and process certain information about its staff members, students, parents, governors, visitors and other individuals in accordance with its legal obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The TRUE Learning Partnership may, from time to time, be required to share personal information about its staff or students with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all Trust Board members, 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 imperative, and The TRUE Learning Partnership 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 and the DPA, 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.

Signed by:

_____ Chief Executive Officer (CEO) Date: _____

_____ Chair of Trust Board Date: _____

1) Legal framework

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

- The General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (DPA)
- 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

1.2. This policy will also have 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

1.3. This policy will be implemented in conjunction with the following other School and Trust policies:

- Privacy notices (staff & students)
- E-Safety Policy
- Acceptable Usage
- Freedom of Information Guidance

2) Scope and Application

2.1. This policy applies to all staff employed by The TRUE Learning Partnership and sets out what we expect from staff. Compliance with this policy is mandatory and any breach of this policy may result in disciplinary action.

2.2. Any external organisation and/or persons(s) working on behalf of the Trust are also required to comply with this policy.

2.3. The DPO is responsible for overseeing this policy and developing related policies and guidelines where applicable.

2.4. Employees are responsible for:

- Ensuring that they collect, store and use any personal data in accordance with this policy; and
- Informing the Trust of any changes to their personal data, such as a change of address

2.5. Employees must contact the DPO with any questions about the operation of this policy or the GDPR or the DPA or if they have any concerns that this policy is not being or has not been followed. In particular, employees must always contact the DPO in the following circumstances:

- if they are unsure that they have a lawful basis to use personal data in a particular way;
- if they need to rely on or capture consent;
- if they need to draft a privacy notice;
- if they are unsure about how long personal data should be kept for;
- if they are unsure about what security measures they need to implement to protect personal data;
- if there has been a data protection breach;
- if they need any assistance dealing with any data protection rights invoked by an individual;
- if they need to transfer personal data outside of the European Economic Area;

- whenever they are engaging in a new activity which may affect privacy rights of individuals; or
- if they need help with any contracts or other areas in relation to sharing personal data with third parties.

3) Applicable data

3.1. 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, e.g. names (including initials), identification numbers, a username, an IP address or a job description. 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.

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 including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health and sex life or sexual orientation. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4) Principles

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

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

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

4.3. How the Trust aims to comply with each of the data protection principles is set out in more detail below.

5) Accountability

5.1. **The TRUE Learning Partnership** will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

5.2. The Trust will provide comprehensive, clear and transparent privacy policies.

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

5.4. Internal records of processing activities will include the following:

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

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

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.
- Regularly (annually) training employees on data protection law, this policy, any related policies and any other data protection matters. The Trust will maintain a record of training attendance by employees. All new starters will receive training on data protection.

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

6) Data protection officer (DPO)

6.1. A DPO will be appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR, the DPA 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.

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

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

6.4. The DPO will report to the highest level of management of the Trust, which is the CEO and the Trust Board.

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

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

7) Lawful processing

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

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

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the trust in the performance of its tasks.)

7.3. Special categories of data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

8) Consent

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

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

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

8.4. The Trust ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

8.5. Consent 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.

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

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

9) The right to be informed

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

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

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

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries 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.

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

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

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

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

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10) The right of access

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

10.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

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

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

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

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

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

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

10.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

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

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

10.12. Personal data about a child belongs to that child, and not the child's parents. For a parent to make a SAR on behalf of their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent.

10.13. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents on behalf of students at the Trust may not be granted without the express permission of the student.

10.14. Employees must immediately forward any SAR to the DPO.

11) The right to rectification

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

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

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

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

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

11.6. Employees must forward any request for rectification received immediately to the DPO.

12) The right to erasure

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

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

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

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

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority

- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

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

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

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

12.7. Employees must forward any requests for erasure immediately to the DPO.

13) The right to restrict processing

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

13.2. In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

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

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

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

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

13.6. Employees must forward any requests for the restriction of processing immediately to the DPO.

14) The right to data portability

14.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
14.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
14.3. The right to data portability only applies in the following cases:

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

14.4. Personal data will be provided in a structured, commonly used and machine-readable form.
14.5. The Trust will provide the information free of charge.
14.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.
14.7. The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.
14.8. In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual.
14.9. The Trust will respond to any requests for portability within one month.
14.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.
14.11. Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.
14.12. Employees must forward any requests for data portability immediately to the DPO.

15) The right to object

15.1. The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
15.2. Individuals have the right to object to the following:

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

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

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

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

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

15.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Trust is not required to comply with an objection to the processing of the data.

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

15.7. Employees must forward any objections to processing to the DPO immediately.

16) Privacy by design and privacy impact assessments

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

16.2. 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.

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

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

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

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV.

16.7. 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

16.8. 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.

17) Data breaches

Although The TRUE Learning Partnership takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen.

Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space)
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the Trust

However the breach has occurred, the following steps should be taken immediately:

1. **Internal Notification:** Individual who has identified the breach has occurred must notify the DPO immediately. A record of the breach should be created using the following templates (Appendix 3):
    a. Data Breach Incident Form
    b. Data Breach Log
    c. Evidence Log

2. **Containment:** DPO to identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** DPO to establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. **Assess the risks:** Before deciding on the next course of action, DPO to assess the risks associated with the data breach giving consideration to the following, which should be recorded in the Data Breach Notification form (Appendix 3):

    a. What type of data is involved
    b. How sensitive is it?
    c. If data has been lost/stolen, are there any protections in place such as encryption?
    d. What has happened to the data?
    e. What could the data tell a third party about the individual?
    f. How many individuals data have been affected by the breach?
    g. Whose data has been breached?
    h. What harm can come to those individuals?
    i. Are there wider consequences to consider such as reputational loss?

5. **Notification to the Information Commissioners Office (ICO):** Following the risk assessment in step 4, the DPO should notify the ICO within 72 hours of the identification of a data breach

if it is deemed that the breach is likely to have a detrimental effect on individuals. This might include if the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social disadvantage.

The DPO should contact ICO using their security breach helpline on 0303 123 1113, option 3 (open Monday to Friday 9am-5pm) or the ICO Data Breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Notification to the Individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. If it is determined that the breach is likely to result in a high risk to the rights and freedoms of the individual(s) then they must be notified by the Trust

7. **Evaluation:** The DPO should assess whether any changes need to be made to the Trust processes and procedures to ensure that a similar breach does not occur.

8. A flow chart detailing the process for any identified breaches is attached in **Appendix 2**

18) Data security

The Trust will keep personal data secure by taking appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage. In particular:

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

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

18.3. 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.

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

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

18.6. All electronic devices are password-protected to protect the information on the device in case of theft.

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

18.8. Staff and governors will not use their personal laptops or computers for Trust purposes.

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

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

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

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

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

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

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

18.15. 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.

18.16. 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.

18.17. The TRUE Learning Partnership takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.18. The Director of Business and Operations is responsible for continuity and recovery measures are in place to ensure the security of protected data.

18.19. Employees must follow all procedures and technologies the Trust puts in place to maintain the security of all personal data from the point it is collected to the point it is destroyed.

18.20. Employees must also comply with all applicable aspects of the Trust's [Acceptable Usage Policy] and not attempt to circumvent the administrative, physical and technical safeguards the Trust implements and maintains in accordance with the GDPR and the DPA.

18.21. The Trust will introduce a protective marking scheme to ensure that all paper based data is coded and stored according to the protection it requires based on Impact Levels:

Impact level	Impact	Colour Code	Encrypted USB device	Example
IL0–Not Protectively Marked	No harm or embarrassment will occur if items become public knowledge		Yes	Newsletters, public information
IL1- Unclassified			Yes	Generic letters to parents containing no personal data
IL2–PROTECT	Some harm or embarrassment will occur if items become public knowledge		Yes	Basic student information such as name and address
IL3–Restricted	Harm or embarrassment will occur if items become public knowledge		Yes	Sensitive Student information such as ethnicity or FSM status
IL4-Confidential	Serious harm or embarrassment will occur if items become public knowledge		No	Highly sensitive student data relating to child protection

When data is sent electronically and is classified as Red (Restricted or Confidential), appropriate encryption must be used.

The TRUE Learning Partnership will use the IRMS Information Management Toolkit for Schools Retention Schedule (Appendix 1) to ensure appropriate measures are taken to mitigate the risk of disclosure of each information asset.

19) Publication of information

19.1. The TRUE Learning Partnership publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

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

19.3. The TRUE Learning Partnership will not publish any personal information, including photos, on its website without the permission of the affected individual.

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

20) Personal information to 3rd parties

20.1. **Information sharing with professionals working with children**. Information sharing between professionals is vital to ensure the wellbeing of children. The Trust will follow the "7 golden rules of information sharing" described by the DfE:

- Remember that the GDPR is not a barrier to sharing information
- Be open and honest with the person or family
- Seek advice if you are in any doubt
- Share with consent where appropriate
- Consider safety and well-being
- Necessary, proportionate, relevant, accurate timely, and secure
- Keep a record of your decision and reasons
- Unauthorised disclosure of personal data is a criminal offence and will likely lead to disciplinary action
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277834/information_sharing_guidance_for_practitioners_and_managers.pdf

20.2. Investigation of a crime

The Trust will treat requests for information from an official bodies related to criminal or taxation purposes under The Law Enforcement Directive. The Trust requires the requestor to complete the Request for Personal Data form (Appendix 4).
Requests from the police will be countersigned by a person no lower than inspector. For requests from other organisations other than the police, the form will be countersigned by a person of a higher position within the organisation than the person making the request.
The decision re access will be made by the Head teacher. Generally, the Trust reserves the right not to release the data but there may be situations such as the receipt of a court order that requires the Trust to release the information.

20.3. Disclosure of non - personal information / FOI Requests

The Trust as a public authority is subject to The Freedom of Information Act 2000 and all requests for information that is not personal information must be treated as a Freedom of Information request. FOI requests must be fully responded within 20 (Trust) working days by law. The information will be provided unless the Trust can provide an exemption under the FOI Act. For more details, The TRUE Learning Partnership's Freedom of Information guidance can be found in Appendix 5.

A more detailed guide to FOI exemptions is here:
https://ico.org.uk/media/for-organisations/documents/1642/guide_to_freedom_of_information.pdf

20.4. Other Circumstances

If the Trust or any working on the Trust's behalf becomes aware of a staff safety issue with regards to one of our students or parents, the Trust will share that information with the appropriate teams and/or individuals to ensure the safety of all concerned.

The Trust may also share personal data in some circumstances with other agencies. We will obtain the necessary consents before referring students to another agency where we are required to do so.

The Trust will sometimes need to share personal data with suppliers and/or contractors who enable the Trust to provide services to students and staff – e.g. IT companies or energy suppliers. The data shared is limited to the specific information the supplier requires in order to carry out their service as well as any additional information that ensures the Trust fulfils our health and safety obligations to the people carrying out the work. The Trust will ensure that suppliers handle this data correctly through the contract terms and the Trust will only use suppliers and/or contractors that comply with the GDPR and the DPA.

The Trust will be responsible for the fair and lawful processing of personal data shared with third parties and will make sure this occurs through data sharing agreements, either in contracts or as standalone agreements.

The Trust will also share personal data with law enforcement and government agencies or public bodies where it is legally required to do so or for the prevention or detection of crime and/or fraud. Examples include:

- The prevention or detection of crime and/or fraud;
- The apprehension or prosecution of offenders;
- The assessment or collection of tax owed to HMRC;
- In connection with legal proceedings;
- Where the disclosure is required to satisfy safeguarding obligations; or
- Research and statistical purposes provided personal data is sufficiently anonymised or consent has been provided.

The Trust may also share personal data where necessary with emergency services and local authorities where it is necessary for them to respond to an emergency situation that affects any of the Trust's students or staff.

21) CCTV and photography

21.1. The CCTV Code of Conduct explains the rationale fully for use of CCTV on the Trust's site.

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

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

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

21.5. All CCTV footage will be kept for six months for security purposes; the Director of Business and Operations is responsible for keeping the records secure and allowing access.

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

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

21.8. Precautions are taken when publishing photographs of students, in print, video or on the Trust/ School website.

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

22) Data retention

22.1. Data will not be kept for longer than is necessary and in accordance with the Trust's retention schedule (see **Appendix 1**).

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

22.3. 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.

22.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained in accordance with the Trust's retention schedule (see **Appendix 1**).

23) DBS data

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

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

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

24) Automated Biometric Recognition Systems

24.1 Where the Trust uses students' biometric data as part of an automated biometric recognition system (for example, using finger prints to receive school dinners), we will comply with the requirements of the Protection of Freedoms Act 2012.

24.2 Parents will be notified before any biometric system is put in place or before their child takes part in it. The Trust will get written consent from at least one parent before any data is taken from the child and processed.

24.3 Parents and students can opt out of the biometric system at any time, and the Trust will make sure their data is deleted.

25) Policy review

25.1. This policy is reviewed every **two years** by the **DPO** and the **Headteacher**, and ratified by the Governing Body

The next scheduled review date for this policy is **May 2020**.

Appendix 1
Information Management Toolkit for Schools

A full retention schedule is outlined in a separate document. This retention schedule is based on guidance from the Information and Records Management Society:
https://cdn.ymaws.com/irms.org.uk/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

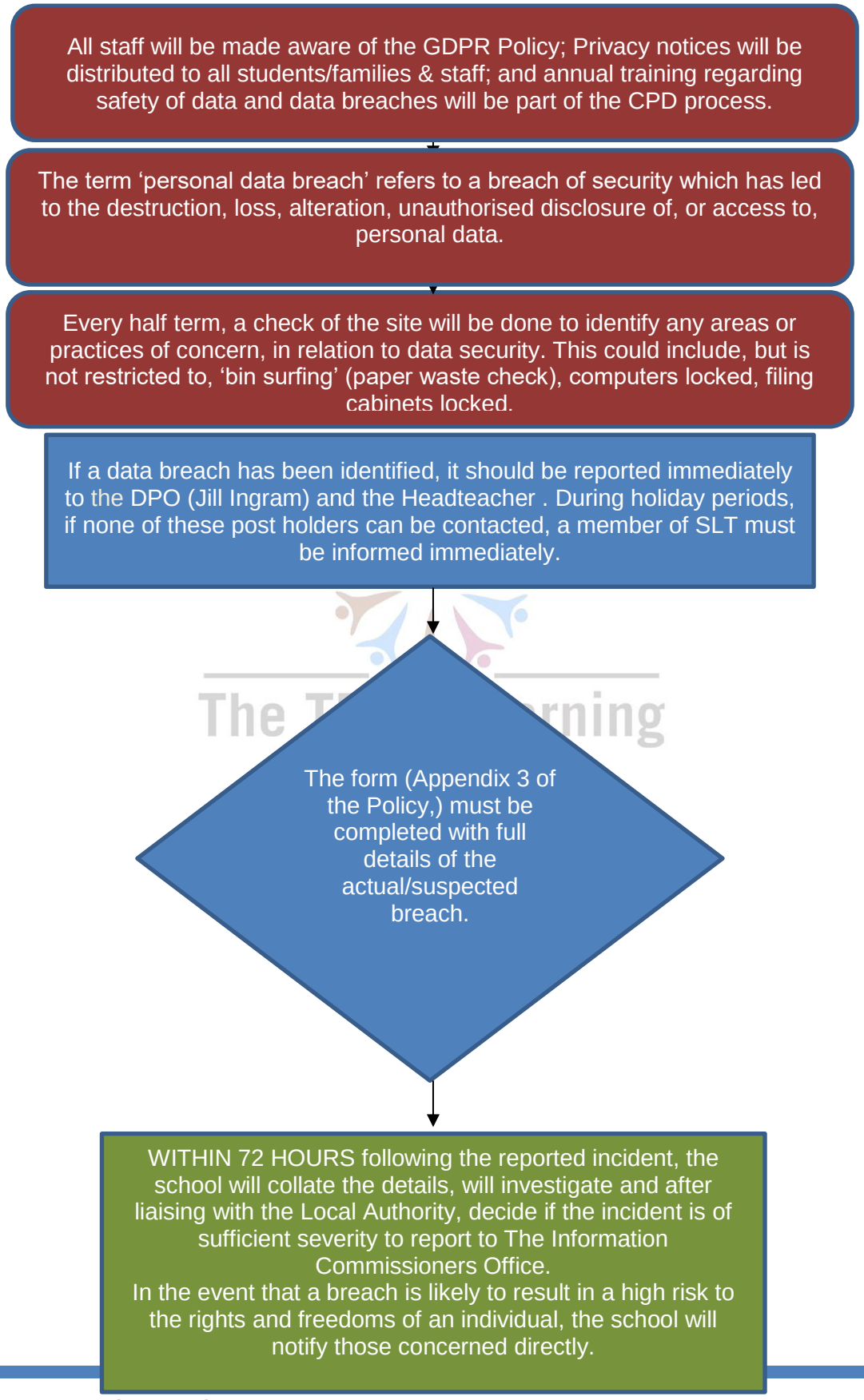
The Data Protection Officer is Mrs Jill Ingram. She is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. This includes:

Owning and updating this policy
Appointing Information Asset Owners (IAOs) and ensuring appropriate staff take ownership of the retention and storage of data in their area of work
Advocating information risk management and raising awareness of information security issues
Decide if a security incident is of sufficient severity to report to the information Commissioners Office.

*Information Asset Owners are responsible for:
Ensuring the information is used for the purpose it was collected
How information has been amended or added to over time
Who has access to protected data and why
Ensuring paper and electronic data is stored in accordance with the IRMS Information Management Toolkit for Schools Retention Schedule, and that all electronic data is sent safely and securely as outlined in the Protective Marking Scheme (Page 18 of this Policy)
Familiarising themselves with the IRMS Retention Schedule and the Retention Guide displayed in offices.

*Information Asset Owners may include the Head Teacher, Sims Manager, Data Manager, Admin staff.

Appendix 2
Procedures for identifying and reporting of data breaches



Appendix 3
Data Breach Incident Form

Part A: Breach Information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of Report:	
Time of Report:	
Description of Breach:	
Initial Containment Activity:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Yes / No Electronic Data: Yes / No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Yes / No Political opinions: Yes / No Religious or philosophical beliefs: Yes / No Trade union membership: Yes / No Data concerning health or sex life and sexual orientation: Yes / No Genetic data: Yes / No Biometric data: Yes / No
Were any protective measures in place to secure the data (e.g. encryption):	Yes / No If yes, please outline:
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	

Whose data has been breached:	
What harm can come to those individuals:	
Are there wider consequences to consider e.g. reputational loss:	

Part C: Breach Notification

Is the breach likely to result in a risk to people's rights and freedoms?	Yes / No If Yes, then the ICO should be notified within 72 hours.
Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms?	Yes / No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data:	
Relevant governors/trustees to be notified:	Names:
	Date Notified:
Notification to any other relevant external agencies:	External agencies:
	Date Notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	

Data Breach Log

Date Reported:	Notified By:	Reported To:	Description of Breach:	Notification to ICO:	Notification to Individual(s)	Further Actions to be taken:	Reviewed by:
				Yes/No	Yes/No		
				Yes/No	Yes/No		
				Yes/No	Yes/No		

Appendix 4

Details of organisations who we share data

Details of data	Internal	External	type

Appendix 5

THE TRUE LEARNING PARTNERSHIP
Freedom of Information Guidance

Our obligations under the Freedom of Information Act:

The Freedom of Information Act and related legislation gives the public the right to be told if information is held (this is the Trust's duty to confirm or deny) and the right to have access to it. Anyone can make a freedom of information request; they don't need to say why they want information and we cannot ask them.

The Information Commissioners advice is that any written request for information should be dealt with as a freedom of information request; the query should be dealt with as soon as possible with a response sent within a maximum of twenty working days. Requests for environmental information may be made verbally.

The Trust will deal with requests as soon as possible; they will not be left until the time limit is about to expire.

What is a request?
Requests should be in writing and give an address to respond to; email and fax are acceptable.

Verbal requests are not covered by FOI. However, we have a duty to provide reasonable assistance and advice. It is considered good practice to offer to help write the person's request down and clarify what information they want if this is necessary.

What information can be requested?
All information recorded and held by the Trust can be requested, even if someone else created it and we do not 'own' it.

This might include information about contractors, suppliers and partner organisations, even if they are not defined as 'Public Authorities 'under the Act.

Information can be in any format and include computer documents, handwritten notes, videos, photographs; even your emails and diaries – this list is not exhaustive.

Exemptions

To ensure proper balance is achieved between the right to know, the right to personal privacy and the delivery of effective government we may decide we cannot release information but we must explain why we cannot supply it and issue a formal 'refusal notice'.
Refusals are limited and must cite one of the exemptions under the terms of the Act.

Instructions on Handling Requests

If the request is straightforward and there is no problem with releasing the information within the 20 working day period then it should be dealt with at school level and the response sent as soon as possible as you usually would.

A copy of our response will be sent to Cheshire East compliance Team in order that they might keep a record and close the log.

There is a quick guide for responding to FOI requests given at the end of this notice.

We will contact the Compliance Unit: foi@cheshireeast.gov.uk about any requests that are at all out of the ordinary and need special attention, for example if:

- The request is unusual
- The request quotes the Freedom of Information Act, Environmental Information Regulations or the Data Protection Act
- The information is not readily available
- We think the information may take a long time to collect
- The information requested needs collating across a number of departments
- We are not sure if the information can be disclosed or if an exemption applies
- It involves a lot of photocopying or printing or additional costs.

Where information is not to be released the Cheshire East compliance Team will prepare and issue the refusal notice and act as a point of contact for the requestor.

Once the refusal notice has been drafted; the service holding the information will need to obtain in writing the permission of their portfolio holder to withhold the requested information.