DATA PROTECTION POLICY

This policy is reviewed every two years by the Trust Board

History of Document

Issue No	Author/ Owner	Date Reviewed	Approved by Trust Board	Comments
i	ALT	Unknown	Unknown	
1	DPO	May 2018	10 May 2018	1st issue post GDPR
2	DPO	June 2018	12 July 2018	Minor amendments
3	DPO	Dec 2018	13 December 2018	Minor amendments
4	DPO	May 2019	23 May 2019	Minor amendments
5	DPO	July 2020	22 October 2020	Amend 4.1.2, Add 5.6 & 5.7, Amend 10.2,10.3,10.7,11.2
6	DPO	Nov 2020	17 December 2020	Amend 2.1. Add 2.4,2.5,3.13. Amend 5.2.1
7	DPO	August 2022	13 October 2022	2.2 Role of DPO
8	DPO	6 March 2023		DPO/Address of Data Controller

1. INTRODUCTION

1.1 The Active Learning Trust Limited ("the Trust") with its academies is registered with the Information Commissioner's Office ("ICO") as a Data Controller, as it is an organisation that collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding.

1.2 This Policy has been produced to ensure that all trustees, staff, pupils and governors are aware of their responsibilities when handling personal information so that personal data is dealt with properly and securely and in accordance with the General Data Protection Regulation ("GDPR") and other related legislation.

1.3 The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.4 This Policy will be updated as necessary to reflect best practice, or amendments made to data protection legislation, and shall be reviewed every two years.

2 RESPONSIBILITY

2.1 The Trust as the corporate body is a Data Controller and the Directors have ultimate accountability for compliance with data protection law.

2.2 The Trust's Data Protection Officer ("DPO") is responsible for overseeing the implementation of this policy, monitoring the Trust's compliance with data protection law and developing related policies and guidelines where applicable.

The DPO will provide an annual report of their activities to the Board of Trustees and report to the Board of Trustees, their advice and recommendations on academy data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust and its academies processes and for the ICO.

The DPO is responsible for informing and advising academies on UK GDPR compliance, coordinating the response to personal data breaches and managing relationships with supervising bodies as and when required.

The Trust Data Protection Officer can be contacted on email – dpo@theictservice.org.uk

2.3 The Headteacher/ Principal in each academy is responsible for:

2.3.1 implementing any policies issued by the Trust regarding data protection and freedom of information

2.3.2 ensuring safe and confidential systems are in place in the school

2.3.3 liaising with the DPO for data protection matters

2.3.4 ensuring all staff are aware of the data protection and freedom of information policies

2.4 Employees are responsible for:

2.4.1 adhering to the terms of this policy

2.4.2 ensuring that all personal information entrusted to them is kept securely

2.4.3 ensuring no personal information is disclosed to any unauthorised third party;

2.4.4 ensuring that their own personal data held by the Trust is kept up to date.

2.4.5 reporting any breaches or risks in data protection to the school's Data Protection Lead and/or the Trust's DPO.

2.5 All new employees and individuals within the scope of the policy are requested to read the policy within the first 4 weeks of joining the Trust. All employees must read the policy every 12 months.

2.6 Individuals may be liable for breaches of the UK GDPR.

2.7 The Information Governance Working Group reports to the Trust's Senior Leadership Team and considers Trust wide cyber security, data protection and information governance matters. Its terms of reference are held at Appendix I.

3. RELATIONSHIP WITH EXISTING POLICIES AND GUIDANCE

3.1 This policy serves as the overarching policy relating to data protection and is supported by more detailed policies covering a range of information and security topics that expand on the high level principles. These include:

- Records Retention Policy
- Subject Access Request Policy
- Data Protection Impact Assessment Policy
- Information Governance Policy
- Records Management Policy
- Data Protection Training Policy
- Data Sharing Policy
- CCTV Policy
- Disaster Recovery Policy

- ICT Security Policy
- Use of Images Policy
- Email Acceptable Use Policy
- Internet, Social Media and E-Safety Acceptable Use Policy

4 PERSONAL DATA

4.1 'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1] such as a name, date of birth, address, NI number, medical information, exam results and an online identifier, such as an IP address.

4.2 A sub-set of personal data is known as 'special category personal data'. This special category data is information that reveals:

4.2.1 race or ethnic origin;

4.2.2 political opinions;

4.2.3 religious or philosophical beliefs;

4.2.4 trade union membership;

4.2.5 physical or mental health;

4.2.6 an individual's sex life or sexual orientation;

4.2.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

4.2 Special Category Data is given special protection, and additional safeguards apply if this information is to be collected and used.

4.3 Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

4.4 The Trust does not intend to seek or hold Special Category Data (previously known as sensitive personal data) about staff or pupils except where the Trust has been notified of the information, or it comes to the Trust's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or pupils are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

5 THE DATA PROTECTION PRINCIPLES

5.1 The six data protection principles as laid down in the GDPR are followed at all times:

5.1.1 personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

5.1.2 personal data shall be collected for legitimate purposes and shall not be further processed in a manner incompatible with those purposes;

5.1.3 personal data shall be adequate, relevant, and limited to what is necessary for the purposes(s) for which it is being processed;

5.1.4 personal data shall be accurate and, where necessary, kept up to date; and all reasonable steps shall be taken to ensure that inaccurate personal data is rectified or deleted without delay;

5.1.5 personal data processed for any purpose(s) shall not be kept in a form which permits identification of individuals for longer than is necessary for that purpose/those purposes;

5.1.6 personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5.2 In addition to this, the Trust is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 8 and 9 below).

5.3 The Trust is committed to complying with the principles in 5.1 at all times. This means that the Trust will:

5.3.1 inform all individuals about how and why we process (collect, store, share, protect and destroy) their personal data through the privacy notices which we issue. The following Privacy Notices have been issued by the Trust:

- Pupil Privacy Notice
- Prospective Parents/Carers Privacy Notice
- Parents/Carers Privacy Notice
- Job Applicants Privacy Notice
- Workforce Privacy Notice
- Emergency Contacts Privacy Notice
- Suppliers Privacy Notice
- Trustees, Governors and Volunteers Privacy Notice
- Visitors Privacy Notice

For pupils, prospective parents and parents/carers, the privacy notices will be made available on a school's website and must be made available as part of any data collection process at the start of each school year - ensuring it is easily accessible at all times. For all job applicants, a copy of the appropriate privacy notice must be recorded on the Trust's recruitment section of its website and with adverts placed on any school's website. For new staff members, the privacy notice must be included as part of an induction pack and be available on the staff notice board / intranet.

All privacy notices will be made available on the Trust's website.

All privacy notices will be reviewed every two years or following a material change in data protection law or regulation.

5.3.2 be responsible for checking the quality and accuracy of the information;

5.3.3 regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Records Retention Policy. Anonymised data can be held indefinitely;

5.3.4 ensure that when information is authorised for disposal it is done appropriately;

5.3.5 ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

5.3.6 share personal information with others only when it is necessary and legally appropriate to do so;

5.3.7 set out clear procedures for responding to requests for access to personal information known as subject access requests;

5.3.8 report any breaches of the UK GDPR in accordance with the procedure in paragraph 12 below.

6 CONDITIONS FOR PROCESSING IN THE FIRST DATA PROTECTION PRINCIPLE

6.1 The individual has given ***consent*** that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

6.2 The processing is necessary for the ***performance of a contract***, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

6.3 The processing is necessary for the ***performance of a legal obligation*** to which we are subject.

6.4 The processing is necessary to protect the ***vital interests*** of the individual or another.

6.5 The processing is necessary for the ***performance of a task carried out in the public interest,*** or in the exercise of official authority vested in us.

6.6 For special categories of personal data, one or more of the special category conditions for processing under data protection law will be met:

6.6.1 The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

6.6.2 The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

6.6.3 The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

6.6.4 The data has already been made **manifestly public** by the individual

6.6.5 The data needs to be processed for the establishment, exercise or defence of **legal claims**

6.6.6 The data needs to be processed for reasons of **substantial public interest** as defined in legislation

6.6.7 The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law

6.6.8 The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law

6.6.9 The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

6.7 For criminal offence data, the Trust will meet both a lawful basis and a condition set out under data protection law. Conditions include:

6.7.1 The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**

6.7.2 The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

6.7.3 The data has already been made **manifestly public** by the individual

6.7.4 The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**

6.7.5 The data needs to be processed for reasons of **substantial public interest** as defined in legislation

7 USE OF PERSONAL DATA BY THE TRUST

7.1 The Trust processes personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be processed in accordance with the data protection principles as outlined in paragraph 4.1 above.

Pupils

7.2 The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

7.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in a school environment.

7.4 The Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Trust, but only where consent has been provided to this.

7.5 In particular, the Trust may:

7.5.1 transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy but only where consent has been obtained first;

7.5.2 make personal data, including special categories of personal data, available to staff for planning curricular or extra-curricular activities;

7.5.3 keep the pupil's previous school informed of his / her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the Trust to their previous school;

7.5.4 use photographs of pupils in accordance with the Trust's Use of Images Policy.

7.6 Any wish to limit or object to any use of personal data should be notified to a Head Teacher/ Principal in writing, which notice will be acknowledged by the school; in writing. If, in the view of the Head Teacher/Principal the objection cannot be maintained, the individual will be given written reasons why the school cannot comply with their request.

Staff

7.7 The personal data held about staff will include name, employee or teacher number, national insurance number, address personal contact details (including telephone and e mail), bank account details and residency history; special categories of personal data including personal and protected characteristics information such as gender, age, ethnicity, disability & health, biometric data etc; contract information (such as start dates, hours worked, post, roles and salary and payroll information); work absence information (such as number of absences and reasons together with related medical information); qualifications (and, where relevant, subjects taught) and training & development and performance records.

7.8 The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

7.9 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

7.10 DBS checks are carried out on the basis of the Trust's legal obligations in relation to the safer recruitment of Staff and the DBS information (which will include personal data relating to criminal convictions and offences) is further processed in the substantial public interest, with the objective of safeguarding children. Retention of the information is covered by the Trust's Records Retention Policy. Access to the DBS information is restricted to those staff who have a genuine need to have access to it for their job roles. In addition to the provisions of the UK GDPR and the Data Protection Act 2018, disclosure of this information is restricted by section 124 of the Police Act 1997 and disclosure to third parties will only be made if it is determined to be lawful.

7.11 Any wish to limit or object to the uses to which personal data is to be put should be notified to the School's Headteacher/Principal who will ensure that this is recorded and adhered to if appropriate. If the School's Headteacher/Principal is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why the academy cannot comply with their request.

Other Individuals

7.12 The Trust may hold personal information in relation to other individuals who have contact with its academies, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles and shall not be kept longer than necessary.

8 SECURITY OF PERSONAL DATA

8.1 The Trust will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this Policy and their duties under the GDPR. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

8.2 For further details as regards security of IT systems, please refer to the Trust's ICT Security Policy.

9. DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES

9.1 The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

9.1.1 to give a confidential reference relating to a current or former employee, volunteer or pupil;

9.1.2 for the prevention or detection of crime;

9.1.3 for the assessment of any tax or duty;

9.1.4 where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);

9.1.5 for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

9.1.6 for the purpose of obtaining legal advice;

9.1.7 for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

9.1.8 to publish the results of public examinations or other achievements of pupils of the Trust

9.1.9 to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips; The legal basis will vary in each case but will usually based on explicit consent, the vital interests of the child or reasons of substantial public interest (usually safeguarding the child or other individuals);

9.1.10 to provide information to another educational establishment to which a pupil is transferring;

9.1.11 to provide information to the Examination Authority as part of the examination process; and

9.1.12 to provide information to the relevant Government Department concerned with national education - the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

9.2 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

9.3 The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

9.4 All requests for the disclosure of personal data must be sent to a School's Headteacher/Principal, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

10. CONFIDENTIALITY OF PUPIL CONCERNS

10.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils. Disclosure for a safeguarding purpose will be lawful because it will be in the substantial public interest.

11. SUBJECT ACCESS REQUESTS

11.1 Anybody who makes a request to see any personal information held about them by the Trust is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.3).

11.2 Individual's full subject access right is to know:

- whether personal data about him or her are being processed
- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom their personal data have been or will be disclosed
- the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored

- where relevant, the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing
- the right to lodge a complaint with the Information Commissioner's Office
- Where the personal data are not collected from the individual, any available information as to their source
- Details of the safeguards in place for any transfers of their data to locations being transferred internationally

11.3 All requests should be sent to a School's Headteacher/Principal and must be dealt with in full without delay and at the latest within one month of receipt or receipt of the additional information needed to confirm identity, where relevant.

11.4 Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or 12 and over but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The School's Headteacher/Principal must, however, be satisfied that:

11.4.1 the child or young person lacks sufficient understanding; and

11.4.2 the request made on behalf of the child or young person is in their interests.

11.5 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the School's Headteacher/Principal must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

11.6 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

11.7 Subject access requests can be made in writing, electronically or verbally. Completion of the Trust's Subject Access Request form by a requestor is the Trust's preferred method.

11.8 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

11.9 Schools can request the assistance of the Trust's Data Protection Officer to assist with the redaction of data before any disclosure takes place.

11.10 Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

12. EXEMPTIONS TO ACCESS BY DATA SUBJECTS

12.1 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

12.2 There are other exemptions from the right of subject access. If we intend to apply any of them to a request, then we will usually explain which exemption is being applied and why.

- Confidential references
- Negotiations between Employer and Employee - the release of the data would prejudice the negotiations
- Management Forecasting/planning - and its release to an individual would prejudice the Trust's business or activities
- Complaints
- Exam Scripts and Marks – this excludes an examiner's comments
- Preventing and Detecting crime – the release of the data would jeopardise the prevention or detection of crime, or the apprehension or prosecution of offenders
- Health Data - Serious Harm Test - safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services
- Education Data – Serious Harm
- Child Abuse Data - safeguarding concerns may contain information about multiple children including siblings and estranged parents; files containing advice from doctors, police or probation services.

13. OTHER RIGHTS OF INDIVIDUALS

13.1 The Trust has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following section sets out how the Trust will comply with the rights to:

13.1.1 object to processing;

13.1.2 rectification;

13.1.3 erasure;

13.1.4 restrict processing and

13.1.5 data portability.

Right to object to processing

13.2 An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest (ground 6.5 above) where they do not believe that those grounds are adequately established.

13.3 Where such an objection is made, it must be sent to the School's Headteacher/Principal and he/she will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

13.4 The School's Headteacher/Principal shall be responsible for notifying the individual of the outcome of their assessment without delay and within a month of receipt of the objection.

Right to rectification

13.5 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the School's Headteacher/Principal and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

13.6 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the Trust's Complaints Policy, or an appeal direct to the Information Commissioner.

13.7 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

13.8 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

13.8.1 where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

13.8.2 where consent is withdrawn and there is no other legal basis for the processing;

13.8.3 where an objection has been raised under the right to object, and found to be legitimate;

13.8.4 where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

13.8.5 where there is a legal obligation on the Trust to delete.

13.9 A School's Headteacher/Principal will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

13.10 In the following circumstances, processing of an individual's personal data may be restricted:

13.10.1 where the accuracy of data has been contested, during the period when the Academy is attempting to verify the accuracy of the data;

13.10.2 where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

13.10.3 where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

13.10.4 where there has been an objection made under para 12.1.1 above, pending the outcome of any decision.

Right to portability

13.11 If an individual wants to send their personal data to another organisation they have a right to request that the Trust provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where the Trust is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the School's Headteacher/Principal and he/she will review and revert as necessary.

14. BREACH OF ANY REQUIREMENT OF THE UK GDPR

14.1 Any and all breaches of the UK GDPR, including a breach of any of the data protection principles shall be reported as soon as it is/they are discovered, to the School's Headteacher/Principal who in turn will advise the Trust's Data Protection Officer.

14.2 Once notified, the Trust's Data Protection Officer shall assess:

14.2.1 the extent of the breach;

14.2.2 the risks to the data subjects as a consequence of the breach;

14.2.3 any security measures in place that will protect the information;

14.2.4 any measures that can be taken immediately to mitigate the risk to the individuals.

14.3 Unless the Trust's DPO concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Trust, unless a delay can be justified.

14.4 The Information Commissioner shall be told:

14.4.1 details of the breach, including the volume of data at risk, and the number and categories of data subjects;

14.4.2 the contact point for any enquiries (which shall usually be the Trust's DPO);

14.4.3 the likely consequences of the breach;

14.4.4 measures proposed or already taken to address the breach.

14.5 If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then either the Trust's Chief Executive, the Trust's DPO or the School's Headteacher, shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

14.6 Data subjects shall be told:

14.6.1 the nature of the breach;

14.6.2 who to contact with any questions;

14.6.3 measures taken to mitigate any risks.

14.7 The Trust's DPO shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Trust's Board and a decision made about implementation of those recommendations.

15. DATA PROTECTION TRAINING

15.1 The Trust will provide data protection training to all new employees as part of their induction programme.

15.2 All employees shall receive a refresher of relevant training every year or following a material change in data protection law or regulation

15.3 The training undertaken by supply staff shall depend upon their role and any assurances they can give about their understanding of data protection laws.

15.4 Each school should keep a record of what training has been undertaken by each data user and their confirmation that they have understood and will adhere to the Trust's data protection processes.

APPENDIX 1 – TERMS OF REFERENCE OF THE INFORMATION GOVERNANCE WORKING GROUP

1.0 Introduction

1.1 It has been recognised that a Trust wide approach to some elements of UK GDPR would be advisable, and as such a Working Group (the "Group") would be formed to discuss Trust wide cyber security and information management matters.

1.2 In addition, it is recognised that the sharing of ideas, thoughts and best practices for individual consideration is an opportunity.

1.3 The Group reports to the Trust's Leadership Team. Any updates or amendments to these terms of reference must be approved by the Trust's Leadership Team.

2.0 Purpose

2.1 ICT & Data Protection related Policies

- To review drafts of relevant ICT & Data Protection related policies and supporting documentation where appropriate and ensure that they are correct and consistent and up to date.
- To review policies prior to consideration by the Trust's Senior Leadership Team and Board of Trustees.

2.2 Cyber Security - Information Risk Register

- To complete a risk assessment via a Risk Register of the Trust's cyber security mechanisms, data protection and GDPR compliance risks which could compromise the privacy of peoples' personal data
- To produce a cyber security – information risk register
- To develop action plans to mitigate the risks
- Assign responsibilities to the actions
- Monitor completion of the actions

2.3 IT Standards

- To undertake IT audits of schools as part of GDPR preparations
- To review the IT infrastructure and cyber security controls operating at each school
- To produce IT Standards and discuss such and timeframes for completion with schools
- To monitor the implementation of the IT Standards

2.4 ICT Disaster Recovery Plan

- Obtain and review schools' Disaster Recovery Plans
- Consider the formation of a Trust wide ICT Disaster Recovery Plan template for schools to complete

2.5 Data Protection Impact Assessments

- To consider and discuss DPIAs where special category data is to be processed by third parties

2.6 Training

- To organise half yearly ICT cyber related training and new IT Standards with internal ICT technicians.

2.7 Data Breaches

- To discuss cyber related security breaches reported on a quarterly basis to the ICO by other organisations

- To discuss improvements to systems should there be a cyber breach within the Trust

2.8 Monitoring

- Regular monitoring of adherence to Trust data protection related and cyber security policies.

2.9 Any Other Business

3.0 Attendance

3.1 The Group will normally be chaired by the Director of Finance and Operations.

3.2 The Trust's Data Protection Officer will take notes of the meetings and circulate such notes and action plans arising from the meetings.

3.3 The Group will comprise of the Trust's Director of Finance and Operations, the Trust's Data Protection Officer and the Trust's ICT Strategic Lead and other nominated individuals with appropriate experience and expertise as nominated by the Trust's Director of Finance and Operations.

4.0 Frequency of Meetings

4.1 The normal frequency of meetings will be termly to be reviewed and increased as required.

4.2 Meeting dates, where possible will normally be scheduled at least termly as a minimum to ensure availability of representatives and meeting rooms. Shorter notice will be given where necessary or appropriate to do so.