The Active Learning Trust

INFORMATION GOVERNANCE POLICY

This policy is reviewed every two years

History of Document

Issue No	Author/Owner	Date Written	Approved by Trust Board	Comments
1	DPO	June 2018	12 July 2018	1st formal issue

1. INTRODUCTION

1.1 Information is a vital asset and plays a key part in corporate governance, school planning and performance management. The Trust recognises the importance of maintaining an appropriate and robust system of Information Governance Management so as to underpin and support schools in the exercise of their functions and in order to maintain public confidence.

1.2 Information Governance is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows the Active Learning Trust ("Trust") and its employees to ensure that information is accurate, dealt with legally, securely, efficiently in order to deliver the best possible service.

2. PURPOSE OF THE POLICY

2.1 The purpose of the Trust's Information Governance Policy ("Policy") is to maximise the value of the Trust's organisational assets by ensuring that data is:

2.1.1 held securely and confidentially;
2.1.2 obtained fairly and lawfully;
2.1.3 recorded accurately and reliably,
2.1.4 used effectively; and
2.1.5 shared and disclosed appropriately.

3. SCOPE

3.1 This Policy applies to all personal information processed by the Trust and its constituent schools.

4. RESPONSIBILITIES

4.1 The Trust Board has ultimate responsibility for setting this Policy.

4.2 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted. Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central Trust.

4.3 It is the responsibility of all staff to process information in accordance with the Data Protection Act 2018 and to adhere to the policies, procedures and guidance that are laid down by the Trust for Information Governance and Security.

4.4 An Information Management & Cyber Security Governance 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.

4.5 The Trust's Data Protection Officer is responsible for monitoring the Trust's compliance with the Policy; submitting a report on the effectiveness of the Policy on an annual basis. The Trust's Data Protection Officer is responsible for submitting any reportable personal information security breaches to the Information Commissioner's Office.

4.6 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted. Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central Trust.

4.7 It is the responsibility of all staff to process information in accordance with the Data Protection Act 2018 and to adhere to the policies, procedures and guidance that are laid down by the Trust for Information Governance and Security.

5. INFORMATION CLASSIFICATION

5.1 The Trust's information is classified in accordance with the harm that might occur to individuals if it was lost, stolen, disclosed to unauthorised persons or corrupted and is classified as:

5.1.1 Highly confidential;
5.1.2 Restricted; or
5.1.3 Unrestricted

5.2 **Highly confidential information** (refer Appendix II) such as special category personal data defined by the General Data Protection Regulation ("GDPR") that reveals an individual's:

5.2.1 race or ethnic origin;

5.2.2 political opinions;

5.2.3 religious or philosophical beliefs;

5.2.4 trade union membership;

5.2.5 physical or mental health;

5.2.6 an individual's sex life or sexual orientation;

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

has significant value for the Trust, and if such personal information was lost, stolen, misused or corrupted, there could be a significant adverse effect on individuals or the Trust. Breaches of information included within the "highly confidential" information category would normally be reportable to the Information Commissioner's Office.

5.3 Only those who explicitly need access to highly confidential information must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles) will be applied as outlined in the Trust's ICT Security Policy.

5.4 When held outside a school, on mobile devices such as laptops, tablets or phones, or in transit, 'Highly Confidential' information must be protected as per the Trust's ICT Security Policy and the Trust IT Standards.

5.5 **Restricted information** (as shown in Appendix III) is subject to controls on access, such as only allowing valid logons from a small group of staff. 'Restricted' information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted. Information defined as Personal Data by the GDPR falls into this category. None intended disclosure or dissemination of this information may incur some negative publicity.

5.6 **Unrestricted information** sometimes called "public information" (as shown in Appendix IV) can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information asset owners (refer paragraph 6.2) to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

6. INFORMATION ASSET REGISTER

6.1 As part of their compliance with the GDPR, the Trust and its constituent schools, together with the Trust's Data Protection Officer are required to discuss and document the personal information assets held in an Information Asset Register ("IAR"). The following should be considered when producing an IAR:

6.1.1 The source of the personal data;

6.1.2 The personal data received;

6.1.3 Where such personal data is stored, its format and who has access;

6.1.4 Why such personal data is required;

6.1.5 The name of the information asset owner;

6.1.6 The technical and organisation's security safeguards in place to protect the personal data;

6.1.7 The names of third party organisations which process personal data on behalf of a school;

6.1.8 The security mechanisms in place when personal data is being transferred outside of the Trust; and

6.1.9 The length of time personal data is retained.

6.2 Each information asset linked to a particular purpose for processing, will be assigned an Information Asset Owner ("IAO"). This is the individual responsible for ensuring that the risks to, and the opportunities for, the information asset are monitored e.g. an examinations officer will be responsible for personal information processed as part of the examinations function of a school. The IAO doesn't need to be the creator or the primary user of the information asset, but they should understand its value to the Trust.

6.3 The results of each school's information audit will be recorded in an excel spreadsheet and reviewed on an annual basis by each school together with the Trust's Data Protection Officer to ensure it is up to date and include all processes undertaken.

6.4 Schools are also required to maintain a pictorial data flow map of personal data flows from/to software which they use. This will be reviewed on an annual basis as per 6.3 above.

7. RECORDS OF PROCESSING ACTIVITIES ("ROPA")

7.1 Article 30 of the GDPR, requires the Trust and its constituent schools to each maintain a ROPA which must document the following:

7.1.1 The name and contact details of the Trust (and where applicable, of other controllers and the Trust's Data Protection Officer);

7.1.2 The purposes of the Trust's processing;

7.1.3 A description of the categories of individuals and categories of personal data;

7.1.4 The categories of recipients of personal data;

7.1.5 Details of the Trust's transfers to third countries including documenting the transfer mechanism safeguards in place;

7.1.6 Retention schedules; and

7.1.7 A description of the Trust's technical and organisational security measures.

7.2 The Information Commissioner's Office also reports that it can be useful to document or link to documentation required for privacy notices. The Trust and its constituent schools will follow such advice and include the following in each ROPA:

7.2.1 the lawful basis for the processing;

7.2.2 the legitimate interests for the processing;

7.2.3 individuals' rights;

7.2.4 the existence of automated decision-making, including profiling;

7.2.5 the source of the personal data; and

7.2.6 records of consent.

7.3 The Trust and its constituent schools will also include reference and links (where appropriate) to the following in their ROPAs:

7.3.1 controller-processor contracts;

7.3.2 the location of personal data;

7.3.3 data protection impact assessment reports where undertaken; and

7.3.4 records of personal data breaches;

7.3.5 information required for processing special category data or criminal conviction and offence data under the Data Protection Act, covering:

7.3.5.1 the condition for processing in the Data Protection Act
7.3.5.2 the lawful basis for the processing in the GDPR
7.3.5.3 link to the Trust's Records Retention Policy

8. RECORDS MANAGEMENT

8.1 Records Management covers the process of creating, describing, using, storing, archiving and disposing of organisational records. Such is covered within the Trust's Records Management Policy.

9. INFORMATION SHARING

9.1 Information Sharing covers the proper governance of information sharing practice across the organisation. It is an essential component given that it deals with business activities involving the potential for sharing personal information about the Trust's students, staff and other stakeholders. Ensuring that the Trust's practice is of the highest standard, meeting with regulatory mechanisms, such as the Data Protection and Human Rights Acts together with the Common Law Duty of Confidentiality, is essential in order to instil confidence amongst those whose personal information is involved in such processes. Information sharing is covered in the Trust's Data Sharing Policy.

10. SUBJECT ACCESS REQUESTS

10.1 Subject Access Requests should be processed in accordance with the Trust's Subject Access Request Policy and associated written procedures and guidance.

10.2 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". The latter 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).

10.3 If employees e.g. teachers are contacted directly by a parent/carer/child e.g. in the playground at the end of the school day, for their personal data or that of their child held by the school, they should advise the individual to contact the school's Headteacher or Business Manager directly on such matter. They must not provide personal data outside the Trust's agreed policy for processing subject access requests. All subject access requests must be processed by a school's Headteacher or Business Manager as per the Trust's Subject Access Request Policy.

11. INFORMATION QUALITY ASSURANCE

11.1 Information quality is generally defined as 'fit for purpose' and all staff need to ensure that data is relevant and accurate. Good data quality means that data is recorded in full, as accurately as possible and in a timely manner. Timely data entry will help avoid discrepancies and inaccuracies. Where it is not possible to record data in real time, this data should be recorded as soon after the event as possible.

11.2 The Trust's Data Protection Officer will conduct information audits on an annual basis as part of an information quality assurance programme, against information held by each school per its IAR to evaluate the information the school is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. This includes the following information:

11.2.1 Paper documents and records
11.2.2 Electronic documents and records
11.2.3 Databases
11.2.4 Sound recordings
11.2.5 Video and photographic records
11.2.6 Hybrid files, containing both paper and electronic information

11.3 Annual information audits may be completed in a number of ways, including, but not limited to:

11.3.1 Interviews with staff members with key responsibilities – to identify information and information flows, etc;

11.3.2 Questionnaires to key staff members to identify information and information flows, etc; and

11.3.3 A mixture of the above

12. REPORTING

12.1 The Trust's Data Protection Officer is responsible for submitting a report on the effectiveness of this Policy to the Trust Board as a minimum on an annual basis.

13. REVIEW

13.1 This Policy will be reviewed every two years by the Trust Board.

APPENDIX I

INFORMATION MANAGEMENT & CYBER SECURITY GOVERNANCE GROUP

TERMS OF REFERENCE

1. Introduction

1.1 It has been recognised that a Trust wide approach to some elements of the General Data Protection Regulation ("GDPR") would be required, and as such a Working Group (the "Group") has been formed to consider the Trust's policies and procedures for cyber security, data protection, information governance and records management.

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

2. 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.
- To maintain a register of DP and ICT related policies so that their review is undertaken at the correct time.

2.2 ICT & Data Protection Risk Registers

- 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 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. 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 Compliance Manager (DPO), the IT Operation Managers of Neale Wade Academy and Cromwell Community College, Trust's ICT Technician and other nominated individuals with appropriate experience and expertise as nominated by the Trust's Director of Finance and Operations.

4. 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.

APPENDIX II INFORMATION CLASSIFICATION

HIGHLY CONFIDENTIAL INFORMATION
If personal information was lost, stolen, misused or corrupted, there could be a significant adverse effect on individuals or the Trust. Such personal data will be limited to authorised persons whose role require it to fulfil their duties, as determined by law, contractual agreement or the Trust's ICT Security Policy. This is a guide not a definitive list.
Special category personal data per GDPR (previously termed sensitive personal data) • race or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • physical or mental health • an individual's sex life or sexual orientation • genetic or biometric data for the purpose of uniquely identifying a natural person • photographs which in some circumstances can indicate ethnicity or religious beliefs • personal data relating to criminal convictions and offences
Personal Information that links one or more identifiable living persons with information about them which, if released would put them at significant risk of harm or distress • financial information e.g. salary, NI number, bank account details, tax, benefit or pensions records • passport number • complete staff/student record for an individual • material related to social services including child protection/safeguarding • disciplinary proceedings
Other • any information which is subject to contractual constraints • information which may be regarded as highly commercially sensitive • legal advice and other information relating to legal action against or by the Trust • information which relates to Trust security matters • passwords to Trust and School systems must NEVER be disclosed to ANYONE

APPENDIX III

RESTRICTED INFORMATION
There could be some adverse effect on individuals or the Trust if personal data was lost, stolen, misused or corrupted. Such personal data will be limited to authorised persons whose role require it to fulfil their duties. This is a guide not a definitive list.
Data that links one or more identifiable living person with information about them which, if released would reveal information about the individual's private life, which may or may not be in the public domain • home address, post code • home or private mobile telephone numbers • date of birth • driving licence number (as this records date of birth and surname) • names of family members or relationships • attendance records
Other • exam papers and assessment material prior to an unseen assessment/exam • routine financial information • key organisational or personnel changes prior to any consultation process • teaching material • software licences negotiated by the Trust
Routine records related to staff and students • Staff/student ID numbers and usernames • Student directory - names, email addresses • Exam scripts and exam marks • References for staff and students (unless it contains data classified as highly restricted)

APPENDIX IV

UNRESTRICTED INFORMATION
Information which is intended to reach most staff and/or students and deals with issues that affect them and their day to day interactions with the Trust/School. There would be little or no adverse effect on individuals or the Trust if such information was lost, stolen, misused or corrupted. This is a guide not a definitive list.
• staff directory – (including names, job titles and work contact details) • trust organisational structure • exam and meeting timetables • personal data which has been anonymised • data agreed by data subjects to be put into the public domain • minutes of meetings of the Trust Board • annual financial statements • information required to be published under the Freedom of Information Act