Alexandra Academy Trust
GDPR Policy

If you need this in an alternative format please contact the Alexandra Academy Trust.

For approval by the Resources committee	Autumn 2021
For Review	Autumn 2024

Signed _____ *(Chair of Resources committee)*

Dated _____

GDPR policy

Trust Mission statement

'Working together to create better futures'

Introduction

The Alexandra Academy Trust will comply with the demands of the General Data Protection Regulation (GDPR), to be known as the Data Protection Act 2018.

Members of staff will gain familiarisation with the requirements of the GDPR either in a staff briefing or as part of their induction.

This policy follows guidance issued by the Information Commissioner's Office (ICO) and the Department for Education (DfE).

The Academy Trust is a Data Controller, as data is processed that is the personal information of pupils, families, staff, visitors and other Academy users.

The Academy Trust is a Data Processor, as it processes data on behalf of other public bodies such as the DfE.

Definitions

Data Processing
The acquisition, storage, processing and transmission of data

Data Subject
Any identifiable person whose data is processed

Consent
Consent must be freely given, specific and an unambiguous indication of the subject's wishes. It must be recorded and available to an audit. A person must be 13 years old in order to record their consent.

Cross-Border Processing
The GDPR covers all EU states and will remain part of UK law. Data cannot be stored beyond the EU and UK borders (the exact borders are those of the European Economic Area)

Sensitive Data
The GDPR/ICO requires that particular care is taken with the following data

- Data regarding children
- Health (physical, mental, genetic)
- Ethnicity
- Religion
- Sexuality
- Performance management and trade union membership

Filing System
Any structured set of personal data, however stored in any format (physical or digital) that can be processed.

Personal Data Breach

A breach of data security leading to the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure, destruction, sale or access to any processed data. Data subjects affected by a data breach must be informed of the breach within 72 hours. Breaches must be reported to the ICO within 72 hours.

Pseudonymisation
The act of making data anonymous. There must be security between pseudonymised data and any data that could re-identify a person.

Password Protection
The act of 'locking' a device or document. The information remains readable beyond the password.

Encryption
The act of encoding all the information beyond a password or code.

Legal Basis
The Academy decides, and registers with the ICO, upon which legal basis it processes data. As a public body with set duties the school uses the following bases for processing and controlling data

Legal basis: **Public Task**

- Admissions
- Attendance
- Assessment
- Pupil and staff welfare
- Safe recruitment
- Staff training
- Performance Management

Legal basis: **Consent**

- Various uses of photographs and moving images
- Trade union membership
- Staff ethnicity, religion and health data (Note the Staff Privacy Statement)
- The use of data to promote the social life of the school community

Legal basis: **Contract**

- When processing is required to carry out the performance of a contract

Personal Data

Anything that might lead to the identification of a person: name, number, characteristics, photograph, correspondence.

Data Portability, Data Subject Access Request

Data subjects (or a child's parents) may request access to a copy of all their data. The school has established an efficient means of accomplishing this task which may not carry a charge and will be completed within 15 working days. Data subjects may request that data is brought up-to-date or made more accurate.[1]

Principles

- Personal data must be processed lawfully, fairly and transparently
- Personal data can only be collected for specific, explicit and legitimate purposes
- Personal data must be adequate, relevant and limited to what is necessary for processing
- Personal data must be accurate and kept up-to-date
- Personal data may identify the data subject only as long as is necessary for processing
- Personal data must be processed in a manner that ensures its security
- Any breaches in data security must be reported to the ICO within 72 hours
- The school must report any breaches caused by third parties who have access to school users' data within 72 hours.
- The school must inform any data subject (person identified in data) where a data breach may have led to the unauthorised access to their personal information [2]

Roles and Responsibilities

The Academy Trust's Privacy Statements set out in detail how the Academy Trust will maintain the security of Academy Trust users' data. The

Acceptable Use Policies set out the duties of the staff and other Academy Trust users in supporting data security.

Within the Academy Trust the security of data is coordinated by Kay Burgess

The Trustee with special responsibility for data security is Mr Alan Guildford.

The Academy Trust has appointed a **Data Protection Officer (DPO),** who has responsibility for overseeing the implementation of this policy and all GDPR related documents. The DPO will monitor compliance, report to the school leadership and support the school with updates and interpretations as the GDPR develops.
The DPO will liaise between the Academy Trust and the ICO and must be informed as soon as is practicable of any personal data security breach.

The DPO will support the Academy Trust in its communication with schools users (children, families, parents/carers, Directors, contractors and visitors) about the Academy Trust's GDPR procedures. This will include the drafting of privacy statements, acceptable use policies and data subjects rights.

Data subject requests should be made in writing to the DPO. The DPO might have to respond to any or all of the following:

- Why the data is processed
- On which basis
- Who has seen it
- How long it will be stored for
- Where the data was sourced
- Whether decisions have been based on the data

Children below the age of 13 do not have the right to make a subject access request, so requests must be made by parents. The Academy Trust may take into account the views of a pupil.

The Academy's DPO is:

Jenny Kyurkchieva of Impero Solutions Ltd
Oak House, Mere Way, Ruddington, Nottingham, NG11 6JS
dpo@imperosoftware.com
0303 123 1113

The DPO's duties are set out in greater detail in the service level agreement and contract held between the Academy Trust and Imperio Solutions. Staff should contact the DPO should they believe that this policy and/or the

privacy statements and/or the acceptable use policies are not being followed.

Data Audit

The Academy Trust will carry out a data audit with support from Imperio Solutions and their technical support company. Within the audit the Academy Trust will record all third parties' compliance with the GDPR if those third parties process data for any Academy Trust users. Such confirmation will, from now on, be an essential part of any contract with third parties when the processing of Academy Trust users' data is involved. The Academy Trust will not share data, or have any data processed, by any third parties who do not confirm their compliance with GDPR requirements.

Preferably companies that process school users' data will have certification to ISO27001.

The audit will also check the security of physical and digital records and devices.

Processing Records

To meet the ICO's recommendation that 'scrupulous records' are developed each school will record its processing of data and the results of its data audit. It will record the ongoing security measures for physical and digital filing systems. Confirmation of compliance by third parties accessing any school user data will be recorded.
In broad terms the Academy Trust will record which data has been processed (including deletions when data should no longer be stored) on which legal basis. Consent replies are recorded within the system.

Sharing Data

Personal data may be shared with third parties to:

- Protect the vital interests of a child
- Protect the vital interests of a member of staff
- To prevent or support the detection of fraud or other legal proceedings
- When required to do so by HMRC

CCTV

CCTV is used to support the safety and security of Academy Trust users. Wherever CCTV is installed, the Academy Trust will adhere to the ICO's code of practice* for its use. Although consent is not required for its use prominent notices inform Academy users that CCTV is used within this Academy site.

**In the picture: A data protection code of practice for surveillance cameras and personal information*

Photographs and Moving Images

Consent is requested from parents/carers and staff for the use of images. Letters requesting consent outline the choices that children and staff may make for the use of their images.

The Academy Trust may seek consent to use photographs for the following purposes:

- To support Academy Trust user welfare (identity and security)
- To celebrate achievement within the classroom
- To celebrate achievement within the Academy Trust
- To celebrate achievement in the printed press
- To celebrate achievement online

The Academy Trust's Specific Data Security Measures - Data Protection by Design

A. All IT systems - mobile devices, laptops, tablets, mobile phones and any device capable of processing data, will be password protected.

B. All IT systems will be kept securely; the server and hard disks will be in a locked cabinet and the server room locked when the Academies are closed and at other times of reduced security; desktop computers and portable devices will be sited/stored in secure places.

C. Staff are expected to ensure the safety of their allocated Academy devices: devices may not be let unattended in cars at any time and they must be kept out of sight if taken home.

D. All passwords must be 'strong;' (at least 8 characters with a mixture of upper and lower case letters, numbers and symbols), the Academy Trust recommends regular changing of passwords.

E. No passwords will be written down or shared; advice is available on the safe storage of passwords.

F. The Academy Trust will devise granulated levels of access as appropriate to staff responsibilities for access to personal data.

G. Devices that are used to process sensitive data and/or are vulnerable to theft will be secured with encryption.

H. All emails containing personal data will use the Egress system which is encrypted

I. All sensitive data will be deleted in a secure manner: physical data will be shredded and digital data will fully deleted with trash/junk emptied regularly. Hard disks no longer required will have the data on them deleted and the deletion certified by the relevant company used for collection/disposal.

J. Only data that is necessary for the effective performance of the individual Academy will be processed.

K. Data protection will be integrated into all appropriate policies and procedures (e.g. staff induction).

L. Staff will be updated with any significant interpretations or developments of the GDPR.

M. The Academy Trust will have data impact assessments in place to protect vulnerable data subjects and sensitive data.

N. Data contained within an email, or attached to an email, will be transferred to a secure folder and the email deleted.

O. Physical data will be kept securely, having regard to the sensitivity of the data and the vulnerability of the data subject e.g. medical data will be accessible to those who need to support an Academy Trust user's needs and located in each academy office.

P. All Academy Trust users will handle personal data with care: it will not be left unattended (unattended computers must be locked), Academy Trust users will not allow others to oversee personal data (screens must be positioned with care); papers must not be left where others can see them.

Q. All computers that might be used to process data will be set to lock (a screensaver will activate) after 10 minutes of inactivity.

R. The Principal and/or the DPO will approve who and how personal data is stored on mobile devices.

S. All digital data that is stored will be backed up on at least a password protected device. Office documents in the 'm' drive are backed up securely offsite using the RBUSS system purchased through CHESS

T. Personally owned devices will not be used for the storage of Academy Trust personal data.

Data breaches

All staff must report to a member of the SLT or the DPO any suspected data breaches (the loss, theft, unauthorised access to data etc.) immediately. It will be for the SLT/DPO to decide whether the suspected data breach warrants reporting to the ICO. NB a data breach would include the accidental sharing of personal data via a wrongly addressed email.

Training

All staff will receive basic training in the requirements of the GDPR. The training will be recorded in the data audit and/or the data processing records. Trustees and Governors will also receive a briefing. Data protection will form a part of pupils' e-safety education. The school will keep staff, Trustees and Governors up to date with guidance, changes and interpretations to data protection law.

Data Protection Impact Assessment

For the Academy Trust's most sensitive data processing activities each school will have completed a DPIA to ensure that the risk to individuals of a data breach is minimised, as should be the risk to the school's reputation.

Staff involved in processing their school's most sensitive data will have to record their reading and understanding of the relevant DPIA.

Monitoring

The DPO will lead the formal monitoring of each school's compliance with the GDPR. Every member of staff, Trustees and Governors share a responsibility to monitor compliance and to report any suspected failures to comply.

Footnotes

1. Data subjects' rights include:
   - The right to be informed
   - The right of access
   - The right to object
   - The right to be forgotten (this might prove impossible in the Academy context)
   - The right of rectification (any inaccurate data must be corrected)

2. In deciding whether to pass on a suspected data breach to the ICO the DPO will consider whether the data breach might affect a person's
   - Reputation
   - Confidentiality
   - Financial wellbeing
   - A loss of control over their data
   - Make them vulnerable to discrimination
   - Their rights and freedoms