The Aspire Academy Trust

Data Handling and Protection Policy

Contents

The Aspire Academy Trust

Data Handling and Protection Policy

Policy aims and objectives

- To meet the statutory requirement for all schools/ academies to have a Data Protection Policy.

- To comply with the requirements of the **'Data Protection Act 1998'** (DPA), **'Data Handling Procedures in Government'** and the wide range of other legislations related to data protection and use. (http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

- To define 'Personal Data' and 'Sensitive Personal Data' and to acknowledge the unique amount of such held within and by the Trust and the consequences of poor handling and management of data.

- To mitigate the risk of personal and sensitive data loss through:
    - Theft
    - A deliberate attack on systems and IT
    - Unauthorised use of personal data by a member of staff
    - Accidental loss
    - Equipment failure

- To minimise the risk to the Aspire Academy Trust and member academies of negative publicity and loss of reputation from such an event and the embarrassment and threat to personal and professional reputations for individuals/ employees.

- To protect the Trust and individuals from disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office.

- To ensure the appropriate use of all forms/ types of personal data and to acknowledge that an increasing amount is being held digitally and therefore accessible remotely across multi-sites.

- To ensure all academies, employees and stakeholders with access to personal data, are aware of their responsibilities to do everything within their power to ensure the security of any material of a personal or sensitive nature when handling, using or transferring personal data and to ensure it cannot be accessed by anyone who does not:
    - have permission to access that data, and/or
    - need to have access to that data.

- To ensure that the Trust and its member academies, train staff on good practice and the contents of this policy and publishes a Privacy Notice for all new and existing parents/ carers and relevant others.

The Aspire Academy Trust

Data Handling and Protection Policy

1. Policy Statements

1.1. The Trust and its member academies will ensure to hold the minimum amount of personal data necessary to enable it to perform its function and for no longer than necessary for the purposes it was collected for.

1.2. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

1.3. All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (See appendix A)

2. Personal and Sensitive Personal Data

2.1. **Personal Data**

2.1.1. Can be held in digital format or on paper records.

2.1.2. It can be defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances, to include:

- Personal information about members of the academy community – including pupils, employees and parents/ carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents or by other agencies working with families or staff members.

2.2. **Sensitive Personal Data**

2.2.1. As above plus information consisting of the following on the data subject:

- racial or ethnic origin
- political opinions, religious beliefs or other beliefs of a similar nature
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- physical or mental health or condition
- sexual life
- a commission, or an alleged commission, any resulting proceedings of an offence, the disposal of such proceedings or the sentence of any court in such proceedings.

3. Responsibilities

3.1. The Trust board has ultimate responsibility for the Trust's data management and security but will delegate the responsibility for such to **ALL** staff and relevant stakeholders but give specific duties to named **Information Asset Owners (IAOs)** to assist with this duty.

3.2. IAOs will be responsible for:

- ensuring systems and procedures are compliant to current legislation and guidance
- managing and addressing risks
- the information held, for how long and for what purpose
- who has access to protected data and why.

3.3. The Aspire Academy Trust will delegate authority and responsibilities as follows:

		Trust Board/ Committee					Responsible Individual					
		Acad	Hub Council	Fin Comm	Board		ASLT Exec P	Company Sec	ICT Mgr	Finance Director	CEO	Trust Chair	Other
Overall responsibility for Data Protection					x								
Data Protection Officer											x		
Appointing IAOs											x		
Registering with ICO and updating policy & legislation								x		x			
Named IAO – Pupil Info and Assessment Data							x						
Named IAO – IT Security, Cloud Hosting, Backups etc									x				
Named IAO – Governance/ minutes								x					
Named IAO – Finance, Contracts and Personnel										x			

4. Registration

4.1. The Academy Trust will register as a Data Controller on the Data Protection Register held by the Information Commissioner every year and an ensure all member academies are listed under the Trust membership.
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

4.2. Certificates of membership will be distributed to each member academy and displayed for all to see.

5. Information to Parents / Carers – the "Privacy Notice"

5.1. In order to comply with DPA, the Trust and member academies will inform parents / carers of all pupils of:

- the data they collect, process and hold on the pupils
- the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed.

5.2. This privacy notice can be passed or directed to new and existing parents / carers through the academy website, prospectus, newsletters, reports or a specific flyer or communication method. (See appendix A)
http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

6. Training & awareness

6.1. The Trust will ensure all staff will receive data handling awareness / data protection training in the aim that all employees are aware of their responsibilities, as described in this policy through:

- New staff inductions
- Staff meetings / briefings / Insets
- Day to day support and guidance from Information Asset Owners

7. Risk Assessments

7.1. Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

7.2. Risk assessments are an ongoing process and will result in the completion of an **Information Risk Actions Form**

8. Secure Storage of and access to data

8.1. The Trust will ensure that ICT systems hide and protect sensitive files from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to the individual.

8.2. Members of staff will not, as a matter of course, be granted access to the whole management information system.

8.3. All users will use strong passwords which must be changed regularly as detailed in the Technical Security Policy. User passwords must never be shared.

8.4. Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used.

8.5. **Trust data must never be stored on an unencrypted and password protected USB stick**

8.6. All other storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

8.7. Personal data can only be stored on Trust equipment (this includes computers and allowable portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal Trust data.

8.8. When personal data is stored on any allowable portable computer system, or removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software and
- the data must be securely deleted from the device, in line with Trust policy once it has been transferred or its use is complete.

8.9. The Trust has clear policy and procedures for the automatic backing up, accessing and restoring all data held on academy systems, including off-site backups (See the Aspire Technical Security Policy).

8.10. The Trust has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Office 365 and Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act.

8.11. The Trust will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

8.12. As a Data Controller, the Trust is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

8.13. All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

8.14. The Trust recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access.

9. Secure transfer of data and access outside of the Trust

9.1. The Trust recognises that personal data may be accessed by users outside of the Trust/ academy, or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive, restricted or protected personal data from the academy or authorised premises without permission.
- USB sticks must never be used.
- Where possible, personal information sent outside of the trust should be shared using encrypted IT systems (Secure website, Encrypted email or shared via Onedrive) and a risk assessment should be carried out.
- The transferring media must be encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of the academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software;
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the Trust in this event. (especially with regards encrypted data being forbidden in most foreign countries)

10. Disposal of data

10.1. The Trust will comply with the requirements for the safe destruction of personal data when it is no longer required.

10.2. The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely.

10.3. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

11. Audit Logging / Reporting / Incident Handling

11.1. It is good practice that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by the Trust IT team, and relevant IAO

11.2. The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy and the following is recorded:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- results in a plan of action for rapid resolution
- a plan of action of non-recurrence and further awareness raising.

11.3. All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office.

12. Use of Cloud Services

12.1. The Trust will always seek parental permission for the use of any cloud hosting services needing an account to be set up for a pupil.

12.2. The Trust remains ultimately responsible for the contract with the provider of the hosting system.

12.3. Therefore, before any contract with such, the Trust will ensure the following points are clarified:

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?
- Who has access to the data?
- Is personal information shared with anyone else?
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that the information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will the data be protected?
- What level of support is offered as part of the service?

13. Appendix A – Privacy Notice Template

Privacy Notice - Data Protection Act 1998

We**,** the **Aspire Academy Trust,** are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school or academy and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well the academy is doing.

This information includes your contact details, assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information.

We will not give information about you to anyone outside the Academy or Trust without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that we hold and/or share, please contact **your Academy administrator or Principal**

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

www.cornwall.gov.uk and
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites, we can send you a copy of this information. Please contact the LA or DfE as follows:

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288