Data Handling Procedure

Contents

1. Introduction

All Acer Trust schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioner's Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

The Data Protection Act (DPA) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and correction. The DPA requires organisations to comply with eight data protection principles, which, among others require data controllers to be open about how the personal data they collect is used.

The DPA defines "Personal Data" as data which relate to a living individual who can be identified

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Link: http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

It further defines "Sensitive Personal Data" as personal data consisting of information as to:

- the racial or ethnic origin of the data subject

- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

2. Policy Statement

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

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

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Acer Trust Privacy Notice)

3. Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff 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 / student 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 / carers or by other agencies working with families or staff members

4. Responsibilities

Each school will appoint a Data Protection Lead (DPL). This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) *for the various types of* data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information as been amended or added to over time

Everyone in the school has the responsibility of handling sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5. Registration

The Acer Trust is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Privacy Notice"
In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers via the school website and letters on arrival at the school. Parents / carers of young people who are new to the school will be provided with the privacy notice through transition documents provided when they join the school.

6. Training & Awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners/School Data Protection Lead

7. Data Protection Impact Assessments (DPIAs)

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.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

8. Secure Storage of and access to data

The school will ensure that systems are set up so that the existence of confidential files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Schools will use a school information

management system to do this. Access to data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. This will be a time period set by each school, but not longer than once per term. User passwords must never be shared.

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 after one hour. Passwords must contain a minimum of 8 characters and contain letters numbers and capitals.

School equipment that has personal data stored on it must not be shared with family members.

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

Memory sticks and portable USB drives must not be used to store personal data

Private equipment (i.e. owned by the users) must not be used for the storage of personal data, but can be used to access cloud storage systems or remote information management systems.

When personal data is stored on any portable computer system, the data must be encrypted and password protected,

- the device must be password protected with a strong password (see above)
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Acer Trust has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

Acer Trust has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud

based data services providers to protect the data, using the ICO guidance as a basis for this: ICO Cloud Computing Guidance

When using a cloud storage system each school will ensure that it meets requirements and will check the following

- 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? Look out for opt in/opt out features
- 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 your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?
- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

Parental permission for use of cloud hosted services
Trust schools will seek consent for use of cloud based IT systems

As a Data Controller, the *Acer 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.

The *Acer Trust* recognises that under GDPR data subjects have a number of rights in connection with their personal data https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

The main one being the right of access. Procedures are in place (see GDPR policy) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know:

if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

9. Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school

- 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; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.
- Care will be taken when transporting hard copies of data, for example markbooks containing sensitive information. These documents will not be left unattended in a car or be accessible to family members in the home

10. Disposal of data

The schools in the trust will comply with the requirements for the safe destruction of personal data when it is no longer required. The DFE toolkit Annex 5.1 guidance on data retention will be used alongside IRMS toolkit for schools will be used to determine the length of time data is stored

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files will be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log of pupil records will be kept and updated annually of all data that is disposed of.

11. Audit Logging / Reporting / Incident Handling

The trust will audit the activities of data users and use GDPRiS as the tool to do this

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of data or breaches of an acceptable use policy, for example.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

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

All significant data protection incidents must be reported through the School Data Protection Lead(DPL) via the Acer Trust DPO to the Information Commissioner's office based upon the local incident handling policy and communication plan.

12. Use of Biometric Information

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- Each School will obtain the written consent of a parent before they take and process their child's biometric data.
- Each school will provide alternative means for accessing services where a parent or pupil has refused consent.