Data Protection and Information Security Policy and Procedure

Contents

1. Purpose

The purpose of this policy and procedure is to ensure compliance of Prenton High School for Girls with all of its obligations as set out in the Data Protection legislation.

2. Data Controller

The Academy is the Data Controller as defined in the Data Protection Act 1998.

3. Notification with the Information Commissioner's Office (ICO)

The Academy notified the ICO, when it was established, using the on-line form
http://www.ico.gov.uk/for_organisations/data_protection/notification/notify.aspx

4. Definitions

4.1. **Personal data** is information that relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and students, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

4.2. **Sensitive personal data** is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on processing sensitive personal data than there are on personal data.

5. Data Protection Principles

The eight core principles of the Data Protection Act are enshrined in this policy in the Academy's commitment that personal data:

- Is processed fairly and lawfully;
- Is obtained only for lawful purposes, and is not further used in any manner incompatible with those original purposes;
- Is accurate and, where necessary, kept up to date;
- Is adequate, relevant and not excessive in relation to the purposes for which it is processed;
- Is not kept for longer than is necessary for those purposes;
- Is processed in accordance with the rights of data subjects under the DPA;
- Is protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- Is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection of the personal information.

6. Fair Processing

The Academy is committed to being clear and transparent about what type of personal information we hold and how it is used. The following 'Privacy Notice for Students and their Parents and Carers' will be published on the Academy Website.

7. Privacy Notice for Students and their Parents and Carers

7.1. Why do we collect information?

7.1.1. The Academy Trust collects information about our students and holds this personal data so that we can:

7.1.1.1. Support each student's learning;
7.1.1.2. Monitor and report on each student's progress;
7.1.1.3. Provide appropriate pastoral care and other support to each of our students; and
7.1.1.4. Assess how well each Student is doing and report on that to the parents.

7.2. What type of information do we collect?

7.2.1. The information will include: personal data such as name and date of birth as well as contact details; educational performance assessments; attendance information; pastoral information. It will also include sensitive personal data such as: ethnicity; special educational needs; behavioural incidents; and medical information that will help us to support each student's education and wider welfare needs at the Academy.

7.2.2. We will also hold personal contact information about parents and carers so that we can get hold of you routinely or in an emergency.

7.2.3. Where CCTV is used by the Academy this will only be for general security purposes in order to protect the students and staff of the Academy.

7.2.4. Student photographs may be included, as part of their personal data and this will be treated with the same level of confidentiality as all other personal data. Photographic images of students used in publically available media such as website, newsletters or the school prospectus will not identify students unless parental permission has been given in advance.

7.3. Do we share this information with anyone else?

We do not share any of this data with any other organisation without your permission except where the law requires it. We are required to provide student data to central government through the Department for Education (DfE www.education.gov.uk) and the Education Funding Agency (EFA www.education.gov.uk/efa). Where it is necessary to protect a child, the Academy will also share data with the Local Authority Children's Social Services and/or the Police.

7.4. Can we see the personal data that you hold about our child?

7.4.1. All students have a right to have a copy of the personal information held about them. As our students are of secondary school age, a request for a copy of the personal information has to be made by a parent or guardian in writing. The only circumstances under which the information would be withheld would be if there was a child protection risk, specifically:

7.4.1.1. The information might cause serious harm to the physical or mental health of the student or another individual;

7.4.1.2. Where disclosure would reveal a child is at risk of abuse;

7.4.1.3. Information contained in adoption or parental order records;

7.4.1.4. Information given to a court in proceedings under the Magistrate's Courts (Children and Young Persons) Rules 1992; and

7.4.1.5. Copies of examination scripts.

7.4.2. If you want a printed copy of the personal data then the Academy will charge the actual cost of providing the copy up to a maximum of a £10 charge. To protect each child's right of confidentiality under law the Academy reserves the right to check the identity of a person making a request for information on a child's behalf. Once any identity check has been completed and any fee due paid, the information will be collected and provided within 40 calendar days.

7.5. Can we see our child's educational record?

7.5.1. All parents are also entitled to a copy of their child's educational record. A request must be made in writing to the Governing Board. The Educational Record includes curriculum, assessment, pastoral and behavioural information that is stored by the Academy. Only information that has come from a teacher or employee of the Academy Trust or an educational professional contracted by the Trust can be considered to form part of the educational record.

7.5.2. The Academy will charge a fee to provide an actual copy of the educational record but this will not be greater than the actual cost of reproducing the information. Once any fee has been received, the Academy will respond to the request within 15 Academy days (21 calendar days excluding any public or Academy holidays).

8. Information Security

8.1. Objective

The information security objective is to ensure that the Academy's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

8.2. Responsibilities

The Headteacher has direct responsibility for maintaining the Information Security policy and for ensuring that the staff of the Academy adheres to it.

8.3. General Security

8.3.1. It is important that unauthorised people are not permitted access to Academy information and that we protect against theft of both equipment and information. This means that we must pay attention to protecting our buildings against unauthorised access. Staff must:
- 8.3.1.1. Not reveal pin numbers or building entry codes to people that you do not know or who cannot prove themselves to be employees;
- 8.3.1.2. Beware of people tailgating you into the building or through a security door;
- 8.3.1.3. If you don't know who someone is and they are not wearing some form of identification, ask them why they are in the building;
- 8.3.1.4. Not position screens on reception desks where members of the public could see them;
- 8.3.1.5. Lock secure areas when you are not in the office;
- 8.3.1.6. Not let anyone remove equipment or records unless you are certain who they are;

8.3.2. Visitors and contractors in Academy buildings should always sign in a visitor's book.

8.4. Security of Paper Records

8.4.1. Paper documents should always be filed with care in the correct files and placed in the correct place in the storage facility.
8.4.2. Records that contain personal data, particularly if the information is sensitive should be locked away when not in use and should not be left open or on desks overnight or when you are not in the office;
8.4.3. Always keep track of files and who has them;
8.4.4. Do not leave files out where others may find them;
8.4.5. Where a file contains confidential or sensitive information, do not give it to someone else to look after.

8.5. Security of Electronic Data

8.5.1. Most of our data and information is collected, processed, stored, analysed and reported electronically. It is essential that our systems, hardware, software and data files are kept secure from damage and unauthorised access. Academy staff must:
- 8.5.1.1. Prevent access to unauthorised people and to those who don't know how to use an item of software properly. It could result in loss of information;
- 8.5.1.2. Keep suppliers' CDs containing software safe and locked away. Always label the CDs so you do not lose them in case they need to be re-loaded;

8.5.2. When we buy a license for software, it usually only covers a certain number of machines. Make sure that you do not exceed this number, as you will be breaking the terms of the contract.
8.5.3. Passwords are a critical element of electronic information security. All staff must manage their passwords in a responsible fashion:
- 8.5.3.1. Don't write it down;
- 8.5.3.2. Don't give anyone your password;
- 8.5.3.3. Your password should be at least 8 characters;
- 8.5.3.4. The essential rule is that your password is something that you can remember but not anything obvious (such as password) or anything that people could guess easily such as your name;

8.5.4. You can be held responsible for any malicious acts by anyone to whom you have given your password;
8.5.5. Include numbers as well as letters in the password;
8.5.6. Take care that no-one can see you type in your password;
8.5.7. Change your password regularly, and certainly when prompted. Also change it if you think that someone may know what it is.
8.5.8. Many database systems, particularly those containing personal data should only allow a level of access appropriate to each staff member. The level may change over time.

8.6. Use of E-Mail and Internet

8.6.1. The use of the Academy's e-mail system and wider Internet use is for the professional work of the Academy. Reasonable personal use of the system in a member of staff's own time is permitted but professional standards of conduct and compliance with the Academy's wider policies are a requirement whenever the e-mail or Internet system is being used. The Academy uses a filtered and monitored broadband service to protect our students. Deliberate attempts to access websites that contain unlawful, pornographic, offensive or gambling content are strictly prohibited. Staff discovering such sites on the system must report this to their line manager immediately. The Headteacher will ensure that the sites are reported to the broadband provider for filtering.

8.6.2. To avoid a computer virus arriving over the Internet, do not open any flashing boxes or visit personal websites;

8.6.3. Do not send highly confidential or sensitive personal information via e-mail;

8.6.4. Save important e-mails straight away;

8.6.5. Unimportant e-mails should be deleted straight away;

8.6.6. Do not send information that breaches the Data Protection Act by e-mail. Do not write anything in an e-mail which could be considered inaccurate or offensive, and cannot be substantiated.

8.7. Electronic Hardware

8.7.1. All hardware held within Academy should be included on the asset register;

8.7.2. When an item is replaced, the register should be updated with the new equipment removed or replaced;

8.7.3. Do not let anyone remove equipment unless you are sure that they are authorised to do so;

8.7.4. In non-secure areas, consider using clamps or other security devices to secure laptops and other portable equipment to desktops.

8.8. Homeworking Guidance

8.8.1. If staff must work outside of the Academy or at home, all of the 'Information Security' policy principles still apply. However, working outside of the Academy presents increased risks for securing information. The following additional requirements apply:

8.8.2. Do not access confidential information when you are in a public place, such as a train and may be overlooked;

8.8.3. Do not have conversations about personal or confidential information on your mobile when in a public place. Ensure that, if urgent, you have your conversation in a separate room or away from other people;

8.8.4. Certified 2 factor authentication is required in order to gain access to remote log-in in order that confidential documents do not have to be taken off site and data is therefore being held securely on the school servers.

8.8.5. If you use a laptop or tablet or smart phone:

8.8.5.1. Ensure that it is locked and password protected to prevent unauthorised access;

8.8.5.2. Make sure that you don't leave your device anywhere it could be stolen. Keep it with you at all times and secure it when you are in the Academy;

8.8.5.3. Portable devices or memory sticks that contain personal data must be encrypted. Personal data may not be taking off the Academy's site or put onto a portable device without the express permission of the Headteacher. Taking personal data off-site on a device or media that is not encrypted could result in a disciplinary matter;

8.8.5.4. Ensure personal data is not stored on the hard drive;

8.8.5.5. When working on confidential documents at home do not leave them lying around where others may see them; dispose of documents using a shredder;

8.8.5.6. If you are using your own computer, it will be only as a portal to the remote home

access solution. Do not transfer documents and data to your own machine. It is forbidden to use a computer owned by you to hold personal data about students or staff at the Academy.

8.8.5.7. Where possible our software specifications will include the function to audit access to confidential data and attribute access, including breaches of security, to specific users.

8.8.6. The Academy will arrange for all critical and personal data to be backed up to secure on-line (off physical site) storage. If the Academy is physically damaged critical data backups will allow the Trust to continue its business at another location with secure data.

8.8.7. Data backup should routinely be managed on a rolling daily process to secure off-site areas.

9. Disposal of Information

9.1. Paper records should be disposed of with care. If papers contain confidential or sensitive information they must be placed in the confidential bins for secure collection or shredded before disposing of them. Particular care must be taken when selecting papers to be placed in a recycling bin.

9.2. Computers and hardware to be disposed of must be completely 'cleaned' before disposal. It is not enough just to delete all the files.

9.3. It cannot be assumed that simply deleting a file will prevent it being recovered from electronic media. Electronic memory containing personal information or sensitive personal information must be electronically scrubbed or physically destroyed.

9.4. Where a third party contractor holds personal information on behalf of the Academy, for example a payroll provider, the Academy will seek reassurance from the contractor regarding their data protection policies and procedures.

10. Subject Access Requests

10.1. Requests from parents or students for access to personal data or educational records will be dealt with as described in the Privacy Notice for Students and their Parents and Carers.

10.2. Academy Trust staff may have access to their personal data within 40 calendar days of a request and at no charge.

10.3. The Academy Trust will maintain a documented record of all requests for personal information with details of who dealt with the request, what information was provided and when, and any outcomes. The record will be used if there is a subsequent complaint in relation to the request.

11. Sharing Personal Information

11.1. The Academy only shares personal information with other organisations where there is a legal requirement to do so or the organisation has been contracted by the Academy Trust to carry out a function of the Academy.

11.2. The Academy is required, for example, to share information with the Department for Education and the Education Funding Agency. Under certain circumstances, such as child protection, we may also be required to share information with Children's Social Services or the police.

11.3. Because students are of secondary school age, their own right to access their own personal information held by the Academy will be exercised through their parents or carers.

11.4. The Headteacher will be responsible for authorising the sharing of data with another organisation. The principle, in authorising the sharing of data will take account of:

- Whether it is lawful to share it;
- Whether there is adequate security in place to protect the information while it is being transferred and then held by the other organisation;
- The Privacy Notice includes a simple explanation of whom the information is being shared with and why.

11.5. Considerations regarding the method of transferring data should include:

- If personal data is sent by e-mail then security may be threatened. You may need to check that the recipient's arrangements are secure enough before sending the message. The data may also need to be password protected and the password sent separately. You should also check that it is going to the correct e-mail address.
- Circular e-mails sent to parents should be sent bcc (blind carbon copy) so that the e-mail addresses are not disclosed to everyone.
- Similar considerations apply to the use of fax machines. Ensure that the recipient will be present to collect a fax when it is sent and that it will not be left unattended on their equipment.
- If confidential personal data is provided by paper copy it is equally important to ensure that it reaches the intended recipient.

12. Websites

12.1. The Academy website will be used to provide important information for parents and students including our Privacy Notice and our Freedom of Information publication scheme.
12.2. Where personal information, including images, are placed on the web site the following principles will apply:
12.3. We will not disclose personal information (including photos) on a web site without the consent of the Student, parent, member of staff or Governor as appropriate;
12.4. Comply with regulations regarding cookies and consent for their use;
12.5. Our website design specifications will take account of the principles of data protection.

13. CCTV

If the Academy uses CCTV, the Information Commissioners Office will be notified along with the purpose of capturing images using CCTV. The Academy appreciates that images captured on CCTV constitute personal information under the Data Protection Act. CCTV footage may be used as evidence to support the exclusion of a student.

14. Photographs

14.1. The Academy may use photographs of students or staff taken for inclusion in the printed prospectus or other school publications without further specific consent being sought.
14.2. Images recorded by parents using their own personal equipment of their child in a school activity for their own family use are not covered by data protection law.
14.3. All other uses by the Academy of photographic images are subject to data protection.

15. Processing by Others

The Academy remains responsible for the protection of data that is processed by another organisation on its behalf. As part of a contract of engagement other organisations that process data on behalf of the Academy will have to specify how they will ensure compliance with data protection law.

16. Training

The Headteacher will ensure that all staff are adequately trained to understand their responsibilities in relation to this policy and procedures.