Blackpool Aspire Academy

Data Protection Policy

Blackpool Aspire Academy is committed to protect the rights of individuals with regards to the processing of personal data. It has established the following policy to support this commitment.

The Academy will comply with the terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure that personal data is treated in a manner that is fair and lawful. Information and guidance is displayed on the Information Commissioners website. (www.dataprotection.gov.uk)

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

For students this includes names, contact details, gender, dates of birth, unique pupil number (UPN) and so on, as well as other sensitive information such as academic achievements, other skills and abilities, and progress in Academy. It may also include behaviour and attendance records.

Although there may be differences in the type of data held the above circumstances can apply equally to information we may legitimately hold on other individuals such as staff, governors, parents etc.

Data does not necessarily just mean 'electronic' data – it also means 'paper data'.

Day to day management of such matters rests under the control of the Principal.

The Academy has made the due notification with the Information Commissioners Office and our register entry can be found within the register of data controllers.

Individuals should be aware that a breach of this policy could lead to disciplinary action being taken, which depending upon the circumstances involved may result in dismissal.

This policy should be read in conjunction with the Academy's Internet Use Policy and CCTV Policy.

Introduction

The Data Protection Act 1998 (the Act) provides safeguards for handling personal information about living and identifiable individuals and is based upon the eight principles of 'good information handling'.

The Academy has a legal obligation to comply with the Act and does so by applying the eight principles of good information handling to the personal data it collects, stores, uses, discloses and destroys. The eight principles are as follows:

Personal Data must be:-
1. processed fairly and lawfully
2. processed for specified and lawful purposes

3. adequate, relevant and not excessive
4. accurate, and where necessary kept up to date
5. not kept longer than is necessary
6. processed in accordance with the rights of the data subject
7. kept secure
8. transferred only to countries with adequate security

The Academy will issue Privacy Notices to staff, students and parents / guardians in relation to the processing of data held on staff and students.

Access to and Use of Personal Information
Access and use of personal information by Academy staff must only be in the course of their official duties. Use for any other purpose is prohibited.

Deliberate unauthorised access to, copying, destruction or alteration of or interference with any computer equipment or data is strictly forbidden and may constitute a criminal and / or a disciplinary offence.

Data Gathering
All personal data relating to staff, students or other people with whom we have contact, whether held on computer or in paper files, are covered by the act.

Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

- Parents may wish to decline to provide the following information about their child: nationality, country of birth, ethnicity, first language and whether they are the child of someone in the Armed Services. In cases such as this, the school can record such data as 'refused'.

- For these data items, schools should only record information that is provided by a parent / guardian or pupil (where a pupil is deemed mature enough to have capacity to consent to sharing their personal data with others).

- In line with the Equalities Act 2010, schools should avoid selectively asking subsets of parents or pupils who share a particular characteristic to complete this information in a different manner to other parents or pupils. Further information on schools' responsibilities under the Equalities Act is available here.

- Parents are not required to share any documentary evidence of a pupil's country of birth or nationality, and schools should not request to see any child's passport or birth certificate, for the purposes of the census.

- Parents can decide to retract nationality and country of birth information previously provided. Further information on this can be found in our updated guidance.

Data Storage
Personal data will be stored in a secure and safe manner.

Electronic data on the Academy's ICT Network will be protected by appropriate password systems and firewalls operated by the Academy.

Data relating to students names and addresses and their contact details must never be saved onto Academy laptops and / or portable memory sticks. Nor should such information be removed from Academy in any other way eg. paper format. An exception to this is in relation to educational visits where the trip organisers and base contacts are authorised to retain a paper copy of all the necessary contact details. Such information must then be shredded at the completion of the trip.

Any other need that may arise for such information to be taken off site must be referred to the Principal for due consideration and authorisation.

Any other student information such as marks or test results must be password protected if it is to be stored on an Academy laptop and / or portable memory stick.

Emergency contact details for staff may be held by designated line managers to assist in the communication of instructions / information in the event of an emergency. It is the responsibility of designated line managers to ensure that they retain such information in a safe and secure manner.

Staff must take every precaution to ensure that Academy laptops and / or portable memory sticks are kept safe and secure at all times.

Computer workstations / laptops will not be left signed on when not being used.

Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting to be attended to at for example reception. Access to working areas should be restricted to appropriately authorised individuals.

Manual / paper data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data. A clear desk policy should be strived for to reduce the potential risks of unauthorised access.

Particular attention will be paid to the need for security of sensitive personal data.

Passwords for access to ICT equipment must not be written down or disclosed to anyone else.

Passwords should be difficult for others to guess so, for example, family / pets names should be avoided. Passwords should preferably contain a combination of upper and lower case letters and numerals and should be changed regularly.

ICT Back up solutions will be in place to ensure that 'personal' data is not lost. Details of these solutions will form part of our Data Security / Business Continuity Protocol.

Data Checking and Accuracy
The Academy will issue regular reminders to staff and parents to ensure that personal data held is up to date and accurate. Staff should ensure that they advise the Academy of any changes to their personal circumstances such as address, contact numbers, emergency contacts etc. so that Academy records can be updated.

Any errors discovered in records will be rectified and if at any time incorrect information has been disclosed to a third party then the recipients will be advised of the corrected data.

It is the responsibility of those who receive personal information to ensure, so far as possible, that it is accurate, valid and up to date. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Matters of opinion (not fact) must be clearly recorded as such.

Staff should be aware that any information that they record about someone, whether in a handwritten note, in an e mail or a formal document, may be disclosed to that person upon request. If an individual is aware that the information recorded is inaccurate, they must take steps to rectify it.

Data Disclosures

Personal Data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given. **The Academy will ensure that to the best of its abilities that such information will be transmitted to the recipient in a safe and secure manner.**

When requests to disclose personal data are received by telephone it is the responsibility of the Academy to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a main switchboard, to ensure the possibility of fraud is minimised.

The same principles apply for people who personally call to the Academy requesting data. If the person is not known personally then proof of identification should be sought.

Personal Data will not be used in newsletters, websites or other media without the consent of the data subject.

Routine consent issues will where possible be built into Academy's Data Gathering Sheets / Home Academy Agreement processes to avoid the need for frequent requests for consent having to be made.

There may be occasions when we need to disclose information about someone which will usually be in breach of the Act. The Act does however contain exemptions which allow us to override a non disclosure provision in certain circumstances, if the disclosure is in the public interest. For example, when the disclosure is necessary for the prevention or detection of crime or the apprehension or prosecution of offenders and where failure to disclose the information would be likely to prejudice an investigation. Similarly we can also disclose information about someone if the information is urgently needed to protect the vital interests of a person (ie. matters of life or death or the prevention of serious harm to an individual). The decision to use an exemption from the non disclosure provisions of the Act will be made on a case by case basis. Advice will be sought from as deemed necessary. Guidance on Information Sharing can be obtained from the Academy Finance Director.

Subject Access Requests

If the Academy receives a written request from a data subject to see any or all of the personal data that the Academy holds about them this should be treated a Subject Access Request and the Academy will respond within the 40 day deadline for doing so.

Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the Academy will comply with its duty to respond within the 40 day time limit.

Review and Destruction of Data

Personal Data will be reviewed at regular intervals to ensure that it is accurate, up to date and still relevant. If personal data held is no longer needed and there is no legal or other reason for holding the information, it should be destroyed.

Guidance will be sought if there are queries over the retention of records.

September 2016 updated January 2017