SILVER BIRCH ACADEMY TRUST
Data Protection and Data Security Policy

DATE
November 2017

REVIEW DATE
November 2019

Introduction

This policy is intended to clarify the obligations of the Silver Birch Academy under the Data Protection Act 1998 ("the Act"). Everyone has rights with regard to how their personal information is handled. During our activities we will

SILVER BIRCH
ACADEMY TRUST

Silver Birch Academy Trust
Registered in England & Wales
No. 08107310

4 Burnside Avenue
Chingford
London. E4 8YJ

www.sba.london
T: 0208 523 3228
E: info@sba.london

collect, store and process personal information about a number of different groups of people and we recognise the need to treat it in an appropriate and lawful manner.

The types of information that we may be required to handle include details of current, past and prospective employees, pupils, parents, trustees, governors, volunteers, suppliers and other individuals that we communicate with. The information, which may be held on paper, on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how we may use that information.

Silver Birch Academy has notified the Information Commissioner that it processes personal information, and is on the register of data controllers. The Trust will amend the entry if it becomes inaccurate, incomplete or requires renewal.

This policy shall apply in its entirety to all employees including headquarters staff, agency workers, contractors, governors and volunteers who shall be referred to in this policy as "staff".

In this policy "school" means any of the schools within Silver Birch Academy.

This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy will be taken seriously and may result in disciplinary action. Breach of the Act may expose the Trust to enforcement action by the Information Commissioner or fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for employees.

The policy should be read in conjunction with the Freedom of Information Policy, the ICT Acceptable Use and E-Safety Policy.

Responsibilities

All staff are responsible for:

- Reading this policy carefully and making sure that they understand it and complying with it. Failure to do so may result in disciplinary action.
- Checking that any information that they provide to the School about their employment is accurate and up to date.
- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently.

The school cannot be held responsible for any errors unless the staff member has informed the school of such changes.

If and when, as part of their responsibilities, staff collect information about other people (e.g. about a pupil's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with guidance provided to staff.

Definition of Terms

Data is information which is stored electronically on a computer or in certain paper based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a school report) and can include telephone numbers, photographs and CCTV images.

Data controllers are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The academy as a body incorporate the Data Controller under the 1998 Act, and the governors are therefore

ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters. They are the Executive Headteacher, the Trust Business Manager and the Academy Business Manager.

Any member of staff, parent or other individual who considers that the policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the appropriate Designated Data Controller.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers who handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Security

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or
- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
- If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- processed fairly and lawfully
- processed for specified and limited purposes and in an appropriate way
- adequate, relevant and not excessive for the purpose
- accurate
- processed in line with data subjects' rights
- secure

and must not be:

- transferred to people or organisations situated in countries without adequate protection
- kept longer than necessary for the purpose.

Fair and Lawful Processing

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the school), the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Fair and lawful processing of data includes having legitimate grounds for collecting and using the personal data, not using the data in ways that have unjustified adverse effects on the individuals concerned, being transparent about how you intend to use the data and handling personal data only in ways they would reasonably expect.

Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate, and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at least annually afterwards. Inaccurate or out-of-date data should be destroyed. If a data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable.

Where a data subject challenges the accuracy of their data, the school will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the relevant local governing body for their judgement. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

Parents and carers will be asked from time to time to confirm the data held on their child to ensure it is accurate.

Timely Processing

Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

Processing in Line with Data Subject's Rights

Data must be processed in line with data subjects' rights. Data subjects have a right to:

- request access to any data held about them by a data controller
- prevent the processing of their data for direct-marketing purposes
- ask to have inaccurate data amended
- prevent processing that is likely to cause damage or distress to themselves or anyone else.

Data Security

The school has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- confidentiality means that only people who are authorised to use the data can access it
- integrity means that personal data should be accurate and suitable for the purpose for which it is processed

- availability means that authorised users should be able to access the data if s/he needs it for authorised purposes. Personal data should therefore be stored on our central computer system instead of on individual PCs.

Security procedures include:

- Physical Security: Appropriate building security measures are in place and only authorised persons are allowed in the computer rooms. Disks, tapes, hard drives, memory sticks and printouts are locked away securely when not in use. Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.
- Computer Security: Only authorised users are allowed access to computer files and password changes are regularly undertaken. Computer files are backed up regularly. Data users should ensure that individual monitors do not show confidential information to passers-by and that s/he logs off from their PC when it is left unattended.
- Procedural Security: In order to be given authorised access to the computer systems, staff will have to undergo checks and will sign a confidentiality agreement. Staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal. CD-ROMs and portable drives are physically destroyed when they are no longer required.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the academy is a safe place for everyone, or to operate other academy policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered sensitive under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the academy to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Retention of Data

The academy has a duty to retain some staff and student personal data for a period of time following their departure from the academy, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Dealing with Subject Access Requests

The Act extends to all data subjects a right of access to their own personal data. A formal request from a data subject for information that we hold must be made in writing. A fee may be payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to their headteacher immediately as there are statutory time limits for responding (currently 40 calendar days).

In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

Requests from pupils who are considered mature enough to understand their rights under the Act will be processed as any subject access request as outlined below and the copy will be given directly to the pupil. The Information Commissioner's guidance is that it may be reasonable to adopt a presumption that by the age of 12 a child has sufficient maturity to understand their rights and to make an access request themselves if s/he wishes. In every case it will be for the school to assess on behalf of the Trust whether the child is capable of understanding their rights under the Act and the implications of their actions, and so decide whether the parent needs to make the request on the child's behalf.

Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent unless the school considers the child to be mature enough to understand their rights under the Act, in which case the school shall ask the child for their consent to disclosure of the personal data (subject to any enactment which permits the School to disclose the personal data to a parent without the child's consent). If consent is not given to disclose, the school shall not disclose the personal data if to do so would breach any of the eight data protection principles.

Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry will be made in the school's Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information. Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

Providing Information over the Telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the school In particular s/he should:

- check the caller's identity
- suggest that the caller put their request in writing
- refer the request and the caller's identity details to the Data Protection Compliance Manager or the Headteacher/Head of School

Authorised Disclosures

The school will, in general, only disclose data about individuals with their consent or unless the law requires or allows us to. There are circumstances under which the school may need to disclose data without explicit consent for that occasion including (but not limited to) the following:

- pupil data disclosed to authorised recipients related to education and administration necessary for the Trust to perform its statutory duties and obligations
- pupil data disclosed to authorised recipients in respect of their child's health, safety and welfare
- pupil data disclosed to parents, partners, social care workers, as appropriate in respect of their staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters
- unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the Trust. disclosures required because of a court order or pursuant to an act of Parliament
- disclosures to the Police where the Trust is satisfied that the information is needed to prevent or detect a crime or to catch and prosecute a suspect.

Only authorised and trained staff can make external disclosures of personal data in accordance with the Act. Data used within the schools by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who needs to know the information to do their work.

CCTV

The school uses CCTV in locations around its sites. This is to:

- protect the school buildings and their assets
- increase personal safety and reduce the fear of crime
- support the Police in a bid to deter and detect crime
- assist in identifying, apprehending and prosecuting offenders
- protect members of the public and private property
- assist in managing the school.

Enquiries

General information about the Act can be obtained from:

www.ico.gov.uk.
www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Complaints

If you consider that the policy has not been followed in respect of personal data about yourself or others, you should raise the matter with the relevant Data Protection Compliance Manager at your school.

Monitoring and Review

This policy will be made available on the school's website. Staff will be notified when the policy is reviewed and provided with access to an up to date version of the policy.

Silver Birch Academy will review this policy at least every two years and assess its implementation and effectiveness.