THE ST. CHRISTOPHER SCHOOL

Academy Trust - Special School

SEN Trust Southend

Mountdale Gardens, Leigh-on-Sea, Essex SS9 4AW
Head Teacher: Mrs. J. Mullan

Telephone: (01702) 524193
Fax: (01702) 526761
E.Mail: office@tscs.southend.sch.uk
Web: www.thestchristopherschool.co.uk

Data Information for our Parents / Carers

Contents

.

1.0 Roles and Responsibilities

This information applies to **all staff** employed by SEN Trust Southend, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

1.1 Local Governing Body

The local governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

1.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities can be requested from the school.

The DPO role is fulfilled by:

- SBM Services (UK) Ltd – Telephone 01206 671103. Email: info@sbmservices.co.uk

1.3 Head of School

The Head of School acts as the representative of the data controller on a day-to-day basis.

1.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this document.
- Informing the school of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

1.5 Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

2.0 Collection and Use of Data

Forms used by the school to collect personal data about a pupil will carry a standard Data Protection notice: as follows:

I/We consent to the school (through the Headteacher as the person responsible) obtaining, using, holding and disclosing "Personal data" including "sensitive personal data" (such as medical information), for the purposes of safeguarding and promoting the welfare of our child, and where necessary, for the legitimate interests of the School and ensuring that all relevant legal obligations of the school and ourselves are complied with. I / We give my / our consent to such processing and disclosure provided that at all times any processing or disclosure of personal data or sensitive personal data is done lawfully and fairly in accordance with the Data Protection Act 1998.

The only exception to this is the letter that is sent out with a prospectus to a new enquirer. The following Data Protection notice should be inserted at the bottom of this letter: *"The personal data you supply to SEN Trust Southend*

will only be used in connection with your interest in a school place. It will be held securely in line with the Data Protection Act and will not be passed to third parties. Each school within SEN Trust Southend is registered under the DP Act."

Schools may make use of limited personal data (such as contact details) relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school.

In particular, the school may:

- Make use of photographs of pupils in school publications and on the school website as set out in the photography consent form. (Photographs with names identifying pupils will not be published on the school website etc. without express permission of the appropriate individual. This permission is gained through the completion and signature of the consent form.)
- Make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities.

2.1 Parents who wish to use Photography and/or Video a School Event

Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use, the DPA will not apply, e.g. where a parent takes a photograph of their child and shares it on tapestry.

Generally photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves. By following some simple guidelines, we can proceed safely and with regard to the law.

- Remember that parents/carers and others attend school events at the invitation of the Head of School.
- The Head of School is responsible for safeguarding all pupils and it has been decided that photography and videoing of school performances is not permitted. Recording or photographing would require the consent of all the other parents whose children may be included in the images.
- The Head of School has the responsibility to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.
- Parents and carers must follow guidance from staff as to when photography is permitted and where to stand in order to minimise disruption to the activity.
- Parents and carers must not photograph or video children changing for performances or events.

2.2 Data Sharing Agreements with Third Party Organisations

The St. Christopher School use some third party agencies to offer guidance and support services to pupils on a 1:1 basis. Examples of such services include Connexions, Mencap and some 'counselling' services.

When such services are delivered on school premises, the school has the right to agree to the confidential nature of such a service or, alternatively, the school may insist that the service operates within the school policy of data handling. Parents should be made aware of the type and nature of the services provided on site for transparency reasons. In normal circumstances parents should be informed if their son or daughter has an appointment with a service, unless the school feels it would not be in the best interests of the pupil to do so. More sensitive 'counselling' interventions are treated on a case by case basis taking into account the views of the pupil, if sufficiently mature.

2.3 CCTV Code of Practice

The Data Protection Act 1998 introduced a systematic legal control of CCTV surveillance through the publication of a Code of Practice that came into effect in March 2000. It was updated in July 2000 and again in October 2001.

Since that time it has become a criminal offence to use an un-notified, non-domestic CCTV system to observe or record people in a public or a private place. It is the responsibility of the Data Protection Officer to include CCTV in the schools DP Notification.

The St. Christopher School have signs that make the public aware that they are entering a zone which is covered by surveillance equipment. In addition it is the responsibility of the Data Protection Officer to ensure that procedures are agreed and in place with regard to day to day operation of the system.

A full copy of the Code is available on the Data Protection web site at http://www.ico.org.uk

2.3.1 Access to Images

Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system.

2.3.2 Access to Images by Third Parties

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system. Examples of third parties include enforcement agencies where images recorded would assist in a criminal enquiry and the prevention of terrorism and disorder. In normal circumstances such agencies will supply appropriate paperwork supporting their request. For example a section 29.3 form will be supplied by the Police in normal circumstances. In emergencies where there is an imminent threat or danger appropriate paperwork may be supplied following limited disclosure.

All requests and subsequent actions will be logged including details of data released, completed request forms and timescales.

2.3.3 Access to Images by a Subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act. **There is no right to instant access.**

- A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms for this purpose are contained in the SEN Trust Data Protection policy. The Data Protection policy outlines the Subject Access Request process which should be followed. The Data Protection Officer will respond to the request in line with the timescale contained in the policy and recognise the 30 day limit to provide the data if the request is granted.
- The Data Protection Officer will then view the data and decide in conjunction with the Headteacher if access to the data and/or a copy will be provided to the applicant. If access to the specified data or a copy is to be provided a decision should also be made regarding the need to seek consent or conceal the identity of other parties shown in the images if deemed necessary.
- The Data Protection Act gives the School the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
- Details of all such requests will be logged and details of actions taken recorded in detail on a S.A.R. Process sheet.
- If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

3.0 Subject Access Requests and Other Rights of Individuals

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject Access Requests must be submitted in writing on a Subject Access Request Form (available from the school office).

If staff receive a subject access request they must immediately forward it to the DPO.

3.1 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

3.2 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

3.3 Other Data Protection Rights of the Individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

4.0 Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in SEN Trust Southend's Data Breach Procedure.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

5.0 Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this document.

This information will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the Bill that affect our school's practice. Otherwise, or from then on, this information will be reviewed **every 2 years** and shared with the full Trustee board.