DATA PROTECTION/GENERAL DATA PROTECTION POLICY

Version Control

Date	Version	Reason	Owner	Author
May 2018	Final	Replace old data protection policy	Executive Principal and SEEAT Board	Data Protection Officer

Supporting documents:

Document Retention and Disposal Guidelines
Records Management Policy
Information Asset Register

Data Protection Policy for South East Academy Trust (SEEAT)

Background

The Data Protection Act (DPA) 1998 is the law that protects personal privacy and upholds individual's rights.

The EU General Data Protection Regulation 2016 (GDPR) comes into force on 25 May 2018 and replaces the Data Protection Act 1998. The changes introduced by the GDPR amount to the biggest reform of data protection and privacy law in over two decades. Some of the precise detail as to how the GDPR will be implemented here in the UK has yet to be decided. So, whilst this this policy is a useful starting point, the school should continue to check the Information Commissioner's Office (ICO) website for further guidance.

The DPA/GDPR applies to anyone who handles or has access to people's personal data. SEEAT collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the Trust. This information is gathered in order to enable it to provide education and other associated functions.

The Trust must also let you know how we use your information and this is done through a Privacy Notice for each school issued to pupils and parents. This summarises the information held on pupils, to include why it is held, the third parties to whom it may be passed on to and destruction timelines.

Scope

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This includes names, addresses, telephone numbers and any expression of opinion about an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings and to any biometric information.

The school collects a large amount of personal data including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the DPA/GDPR, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

Compliance with the DPA/GDPR is the responsibility of all members of the school. Any deliberate breach of the DPA or this policy may lead to disciplinary action being taken, or even to a criminal prosecution.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security; Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

GDPR

From 25 May 2018, the Trust will need to be able to demonstrate that it complies with the following principles, which require that personal data is:

- processed in a lawful, fair and transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate, and where necessary, kept up to date
- kept in a form which enables individuals to be identified for no longer than necessary
- processed in a manner that ensures appropriate security

Although the data protection principles are broadly the same, a new concept of “accountability" has been introduced which covers record keeping and being able to demonstrate compliance.

The rights of individuals

The Trust is already familiar with the right of subject access. This right is changing slightly under the GDPR and more is detailed in Appendix 1.

The GDPR also grants individuals additional rights, which include the following:

- right to be forgotten
- right to data portability

Definitions

Personal data

Like the DPA the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – e.g. an IP address – can be personal data.

For the Trust records with personal information, to include HR records, customer lists, or contact details, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, and is personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation but there are now some minor changes.

For example, the special categories data now specifically includes 'genetic data' and 'biometric data' where processed to 'uniquely identify an individual'.

(Data relating to criminal offences and convictions are now addressed separately.)

Data Protection Officers - DPO

Under the GDPR, *'any public body or authority'* is required to appoint a DPO, but there is no clear-cut guidance as to which institutions qualify as such. Until further guidance is published on this point, all academies (and schools which are already subject to Freedom of Information Act legislation) should assume they will be required to appoint a DPO.

Whilst many schools have already appointed a 'data protection compliance manager' or similar, under GDPR, the DPO receives protected employment status and must:

- be suitably qualified, and an expert in data protection law
- be able to carry out the role independently
- report to the highest level of management

The DPO can either be engaged as an employee or a sub-contractor, and one DPO can act as the DPO for a number of public bodies. SEEAT have initially chosen to appoint the Finance & Operations Director as the DPO for the Trust.

Use of Personal Information by the Trust

The Trust will, from time to time, make use of personal information relating to pupils, their parents or guardians in the following ways:

- Could use photographic images of pupils in school publications and on the school website.
- For fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school, including transferring information to any association society or club set up for the purpose of establishing or maintaining contact with pupils.

If you have any concerns, or wish to limit or object to any such use please notify the Head teacher or the DPO in writing.

Consent

Signed consent to take photographs or record images of children will be requested from the parent or carer on enrolment of their child. The purpose for taking any images is to be clearly explained and agreed. Any consent given is to be reviewed on a regular basis (of a period of no more than one year) until such time the child or young person will no longer attend the school in the Trust.

Obtaining an individual's consent to process personal/sensitive personal data or to transfer personal data outside the EU must now be explicit and will become much harder under GDPR. Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent.

Children

The GDPR identifies children as "vulnerable individuals" deserving of "special protection". To that end, the Trust needs to be aware that the new rules introduce some child-specific provisions, most notably in the context of legal notices and the legal grounds for processing children's data.

When dealing with children (i.e. those under 13 years), consent from a child regarding online services will have to be authorised by a parent. Children's "right to be forgotten" will also become stronger.

The school therefore has to review how it seeks, records and manages consent and implement appropriate mechanisms in order to ensure an effective audit trail.

Additionally, systems and procedures should be reviewed to ensure mechanisms are in place to deliver the rights of data subjects under the GDPR, to include the right to be forgotten.

Data Protection by Design and Data Protection Impact Assessments

The Trust has to implement appropriate technical and organisational measures to show that it integrates data protection into its processing activities. It must also understand and put processes in place to conduct Data Protection Impact Assessments to assess the risks on projects/activities that process personal data.

Staff Training

All staff who have access to personal data should receive training in DPA/GDPR following the changes coming into place. The school should also ensure that it keeps records of who has received training and when.

Personal Data Breaches

The Trust will need to revisit its internal procedures for detecting, reporting and investigating personal data breaches. GDPR requires mandatory breach notification to the regulator and in some cases also to affected individuals. Non-compliance can lead to administrative fines of up to €10m and the more serious breaches can lead to fines of up to €20m.

International Data Transfers

Under current data protection law, transfers of personal data outside the European Economic Area (EEA) are restricted and this will continue to be the case under GDPR.

The Trust should review and map any flows of personal data outside the EEA, consider what transfer mechanisms are in place and whether these comply with GDPR or not. This will apply if the School sends personal data outsider the EEA through the use of service providers such as Cloud Service Providers, bulk emailing services, web hosting services or simply communicating with parents or agents overseas.

Breach of the GDPR's rules on data transfers will be subject to maximum level fines of €20m.

General Statement

How, why and where we keep and use data about data subjects is coming under ever closer scrutiny.

The Trust should be aware and prepare for the changes as Ofsted are likely to continue its policy of heavily criticising schools and academies for data protection breaches.

The Trust is committed to maintaining the above principles at all times and will:

- inform data subjects, this could be pupils, parents or staff why they need their personal Information, how they will use it and with whom it may be shared through Privacy Notices
- check the quality and accuracy of the information held
- ensure that information is not retained for longer than is necessary
- when information is authorised for disposal it is securely destroyed
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests from data subjects, to include: access to personal information known as subject access requests, or the right to be forgotten
- train all staff so that they are aware of their personal responsibilities under data protection

- through robust contractual agreements, ensure that all contractors/third party providers, to include cloud providers are aware of their obligations to the school under data protection .

Complaints

Complaints will be dealt with in accordance with the school's complaints policy and any queries should be directed to either the Head teacher or the DPO. The DPO can be contacted by e-mailing dpo@whsg.info

Complaints relating to information handling may be referred to the Information Commissioner's Office.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 03031231113.

Review

This policy will be reviewed as it is deemed appropriate, but at least every 2 years.
The policy review will be undertaken by the Board of the Trust or one of its committees.

Appendix 1

Procedures for responding to subject access requests made under the DPA/GDPR.

Under the DPA/GDPR any individual has the right to make a request to access the personal information held about them.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email**.** If the initial request does not clearly identify the information required, then further enquiries will be made. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

2. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 13 or above) and the nature of the request. The Head teacher/DPO should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

3. A charge can no longer be made for responding to a subject access request (unless particular circumstances apply) and the time for responding to a subject access request is being reduced from 40 days to one month.

4. The DPA/GDPR have exemptions/derogations as to the provision of some information; therefore all information needs to be reviewed prior to disclosure.

5. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained.

6. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

7. If there are concerns over the disclosure of information then additional advice should be sought.

8. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

9. Information disclosed should be clear and legible and should have no codes or technical jargon.

10. The data subject should be consulted when taking into account the mode of delivery. If postal systems have to be used then registered/recorded mail must be used.