Data Protection Policy

in accordance with

General Data Protection Regulation (GDPR 2016)

Data Protection Policy (General Data Protection Regulation 2016)

1 Statement of Policy

1.1 The Constellation Trust needs to collect and use certain types of information about students, their families, employees and with whom it deals, in order to perform its functions. This includes information on current, past and prospective employees, students, persons with parental responsibility, suppliers, customers, service users and others with whom it communicates. The Constellation Trust is required by law to collect and use certain types of information to fulfill its statutory duties and to comply with the legal requirements of the Government.

1.2 Each Headteacher within the Trust is responsible for data and ensuring the school/academy is GDPR compliant. Any breaches should be reported to the Headteacher in the first instance and must then be relayed to the Chief Operating Officer (Data Controller) and the Executive Head/CEO.

1.3 This policy should be read in conjunction with 'Children and the GDPR' https://ico.org.uk/fororganisations/GuidetoDataProtection/GuidetotheGeneralDataProtectionRegulation(GDPR)/ChildrenandtheGDPR

2 Policy Aims

2.1 This policy outlines the Trust's arrangements to access personal information by students, persons with parental responsibility, public and employees in accordance with the General Data Protection Regulation (GDPR 2016).

2.2 This policy will be communicated to all employees and is accompanied by notes of guidance. This policy will be published to employees through the school/academy's normal channels.

2.3 The policy applies to all personal information held by the Trust irrespective of ownership. Personal information is defined for the purposes of this policy as being any information from which an individual can be identified (including Computer storage, Documents, Photographs, CCTV images, Voice, etc.).

3 Scope

3.1 The policy also applies to all contractors and agencies operating on behalf of the Trust or on the Trust premises. For the purpose of this policy, the term 'employee' covers all of these groups.

4 Policy Objectives

4.1 This policy outlines the Trust's approach to ensuring all employees effectively process and manage personal information within set standards, to protect the privacy of individuals and to comply with the principles and requirements of the GDPR and other relevant legislation. All employees complete training on procedures that comply with GDPR, when handling personal information about Students, Parents, Visitors, Clients, Contractors and Employees.

4.2 This policy should be complied with for personal information relating to all individuals whether deceased or living.

4.3 This policy should be read in conjunction with the Data Retention Policy, the Internet Use Guidance, and Freedom of Information Policy.

4.4 The policy and guidelines cover requests for information from individuals for their own personal data. Such requests, defined as subject access requests (SAR's), should be handled in accordance with this policy, in compliance with GDPR 2016.

4.5 A definition of terms is available at Appendix A.

4.6 To promote the effective, consistent and legal processing of personal information by defining a personal information handling policy.

4.7 To ensure that all employees are aware of their responsibilities in relation to the processing of personal information and to the law surrounding its use.

4.8 To ensure that all employees are aware of the consequences of the misuse or abuse of personal information.

4.9 To establish and maintain trust and confidence in the Trust's ability to process personal information.

4.10 To ensure compliance with legislation, guidance and standards relating to the handling of personal information.

5 Monitoring & Review

5.1 The policy and guidelines will be reviewed annually to take into account changes in legislation and to ensure that they remain timely and relevant. Any changes will be publicised through the Information Commissioners Office (ICO) and normal communication channels.

5.2 The effectiveness of the policy will also be assessed through the monitoring of requests for personal information, the Trust's responses to these, and complaints. These events will be collated into an annual report. Where issues of concern arise, then the Information and Security Officer (ISO) and Information Governance Toolkit (IGT) will be approached.

5.3 The policy will be published on the Trust's website and hard copies will be provided upon request.

5.4 An information audit will be conducted every three years by the Trust's administration team and any recommendations complied with, within agreed timescales. This also complies with Section 46 of the Freedom of Information Act.

6 Procedure

6.1 The Trust regards the lawful and correct treatment of personal information as critical to successful operations and to maintaining confidence between those with whom it deals. It is essential that it treat personal information lawfully and correctly.

6.2 The purpose of the GDPR 2016 is to protect the rights and privacy of living individuals. It regulates the processing of personal information including the obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal information and gives rights to those whose information is being processed.

7 Processing Personal Information

7.1 The processing of personal information is defined as encompassing everything that we do with personal information including the sharing, transferring or disclosing of personal information to another organisation or internally.

7.2 Personal information must be processed in accordance with the **six principles** under the GDPR 2016 unless an exemption applies.

7.3 Employees must respect personal information that they have access to and treat it in the manner in which they would expect their personal details to be treated.

7.4 Employees must have regard and respect for the privacy of students, persons with parental responsibility and employees and process their personal information accordingly.

7.5 Access to personal information must be accepted by all to be on a need and a right to know basis.

7.6 Personal Information should be deleted and disposed of under principles of GDPR 2016.

7.7 Personal information will be held securely and be accessible only by those with a need and a right to know. The Headteacher is responsible for ensuring that personal information held at their school/academy is surrounded by appropriate security, i.e. relevant to the sensitivity of the personal information being processed.

7.8 Arrangements and contingencies need to be in place in order to protect personal information from loss due to natural and unnatural disaster, e.g. flood, arson, theft.

7.9 Personal information must not be transmitted or transported externally via manual or electronic means without appropriate security. Portable devices (laptops, CDs, DVD's, USB memory sticks, etc.) which contain personal information must use adequate security measures e.g. encryption, to protect against losses or access by unauthorised persons. Staff wishing to work on personal information externally should request clearance from the Headteacher and Data Controller (DC) and ensure that security measures are in place before such information is transferred. The Data Controller requests that no identifiable collected information will be accessed by laptops unless encrypted. This is because collected data is the responsibility of the Data Controller (see update November 2018 ref. encryption at **www.ico.org.uk**)

7.10 Personal information must be disposed of safely and securely when it has reached the end of its shelf life.

7.11 Personal information will not be passed on to any third party unless any one or more of the following apply (Principles of GDPR 2016):

- Explicit consent is obtained
- The organisation requesting the information has a legal right to the information (e.g. police investigating crime)
- It is a requirement of law
- It is to comply with a court order
- It is necessary to provide educational services
- The Trust believes it is in the subject's own interest
- The Trust believes it is in the overall public interest and in a particular instance this is judged to outweigh the other considerations

7.12 At the point of collection, the data subject will be informed of the purposes for which the information is being collected and processed together with any other relevant details regarding this processing. At this time, where choices are available the child/young person or persons with parental responsibility will be given the opportunity to opt out of the school's non-statutory information processing arrangements, e.g. consent to the taking of images for publicity purposes.

7.13 The Trust will promote good practice in the sharing of information with its partners, government agencies and departments and other public and private sector organisations. All sharing will comply with the GDPR 2016 and the current General Information Sharing Protocol (GISP).

7.14 The quality and accuracy of personal information should be relevant to the purpose for which it is to be used.

7.15 The purposes for which personal information is processed in the Trust will be detailed in the school/academy Data Protection Notification, which will be renewed annually with the Information Commissioners Office. Any changes to purposes must be identified to the Information and Security Officer (ISO) who will submit amendments as required.

7.16 Processing of information for a purpose not reflected in the GDPR 2016 or in the notification must be approved by the ISO or IGT.

7.17 Any inaccurate or misleading information will be checked and corrected as soon as the student or parent brings this to the Trust's attention.

7.18 The rights of data subjects as defined by the GDPR 2016, and specifically their right of access to their own personal information will be complied with fully and given appropriate respect and priority.

8 The Subject Access Request Procedure

See details on 'Manifestly unfounded and Excessive Requests' Sept 2019 at www.ico.org.uk

8.1 Requests by individuals (or their representative) for copies of their own information must be in writing and supported by significant proof of identity. The following originals (not photocopies) are suggested:

- Passport
- Driving License; or
- Birth/Marriage Certificate

The need to check and verify the identity of the requester can be particularly important where that person is a child or someone is purportedly making the request on behalf or in respect of a child.

8.2 Enquirers should be provided with a Subject Access Request Form (see “Guidance”).

8.3 In the event of a Subject Access Request (SAR), the Headteacher will instruct the DC to prepare and redirect all relevant information. This is also to ensure compliance within timescales (see 8.5).

8.4 Information must not be deleted or disposed of, after the receipt of a request, unless requested by the subject. Subjects have the right to have incorrect or inaccurate information corrected.

8.5 Subject Access Requests will be supplied without undue delay or within one month. Where an investigation of a member of staff has commenced and that member of staff has requested Subject Access, the processing of the request should be undertaken as quickly as possible. In the event that a complaint is received regarding a Subject Access Request, the complaint will be addressed following the Trust’s Complaints Procedure. Records of proceedings and decisions made will be kept in order to provide evidence for any external review of the complaint by the Information Commissioner’s Office.

8.6 Requests for personal information held by the Trust about an individual may result in the Trust seeking clarification from the requestor, for example to specify an area of information required, services or timescales. In cases where clarification is sought, the clock stops until the clarification is received and then restarts from where it left off.

9 Training

9.1 All employees in organisations with over 250 staff require training on the GDPR 2016 and personal information handling. New employees will also require training during induction. Training is seen as one measure to help maintain compliance with the GDPR 2016.

10 Security of Personal Data

10.1 Unacceptable use includes:

- unauthorised access to personal information
- unauthorised disclosure of personal information
- unauthorised use of personal information, e.g. use of which the data subject has not been informed/consented to as in GDPR 2016 Law, section 2, page 48 and the Fair Processing Notice); and
- non-adherence to the Trust's policies and local authority’s information-sharing protocols

10.2 Employee, client or student personal information must not be used for:

- any illegal purpose
- any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the Trust into disrepute; or
- any purpose which is not in accordance with the employee's role or job description

(This is not an exhaustive list).

10.3 Employees are required to notify the Headteacher and Chief Operating Officer (Data Controller), if they become aware or suspect that personal information is being misused or handled inappropriately.

11 Non-Compliance with Legislation & Policy

11.1 The Headteacher is responsible for ensuring that employees' responses to requests for personal information remain appropriate and are in accordance with this policy and the GDPR 2016.

11.2 The Headteacher must ensure that instructions they give to employees, relating to requests for personal information and the processing of personal information, comply with GDPR 2016 and Trust policy.

11.3 Employees need to be aware that arrangements need to be in place that avoid parental and visitor contact with personal information to which they do not have a right.

11.4 All employees must be aware of their own obligations with regard to the disclosure and the processing of personal information.

11.5 Employees not complying with this policy or legislation will have matters reviewed and may be dealt with under the Trust's Disciplinary Procedure. In the event of non-compliance by an agency worker, casual worker or contractor, his/her work with the Trust will also be reviewed under the Trust's Disciplinary Procedure, depending upon the circumstances of the case.

Contact details:

Information Commissioner's Office (ICO) **Tel:** 0303 123 1113
01625 545745 **Fax:** 01625 524510

Press and Media enquiries: Tel: 020 7025 7580
Web address: www.ico.org.uk

By post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

By email: If your enquiry is about a new or existing notification under the GDPR 2016, please email notification@ico.gsi.gov.uk. You may find it helpful to read more about notification and the need to notify before sending your enquiry.

Appendix A

Definitions

(a)	**Personal Information**
	Information relating to a living individual who can be identified from that information or from other information in possession of the organisation. This is information that affects a person's privacy whether in their personal or family life, business or professional capacity and includes the name, address and telephone number of an individual. It will also include information on a person's medical history, an individual's salary details and includes expression of opinion about the individual and of the intentions of the organisation in respect of that individual. Personal information also includes CCTV images and photographs which enable the identification of an individual
(b)	**Special Categories of Personal Information**
	Is defined in the Act as racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal convictions (see update November 2019 www.ico.org.uk)
(c)	**Data Subject**
	Any living individual who is the subject of personal information held by an organisation e.g. a pupil, parent, member of school staff, council employee, agency worker, casual worker, customer, client, member of the public, partnership worker, councillor
(d)	**Processing**
	Any operation relating to information including: organising, retrieving, disclosing or otherwise making information available, deleting, obtaining, recording, altering, adding to, or merging
(e)	**Third Party**
	Any individual or organisation other than the information subject, the information controller or its employees or agents