Data Protection Policy

Policy Scope

The Confederation of School Trusts (the Group) and all its subsidiaries are Data Controllers for the purposes of the EU/UK General Data Protection Regulation (GDPR).

The Group includes:

- Confederation of School Trusts (Company number 05303883)
- CST Professional Development Limited (Company number 10354936)
- National Teacher Accreditation Limited (Company number 08650911)

Each entity are data controllers of their own information. The Group collects and uses certain types of personal information about the following categories of individuals:

- current, past and prospective employees;
- Volunteers including Trustees/Directors;
- Members/service users;
- Prospective members;
- Donors;
- Suppliers, including Consultants
- Early Career Teachers (ECTs)and their induction tutors/ induction leads and headteachers
- and other individuals who come into contact with the Group.

The Group will process this personal information in the following ways:

- to comply with statutory and contractual obligations relating to employment and engagement of consultants/contractors;
- To comply with contractual obligations to provide a service to our members;
- to comply with statutory and contractual obligations relating to ECT induction
- to comply with statutory and other legal obligations relating to safeguarding;
- to comply with third-party processing activities in respect of the service or legal requirements;
- See Appendix 1.0

Policy Objectives

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with GDPR and other related legislation. It will apply to information regardless of the way it is used or recorded and applies for as long as the information is held.

The GDPR applies to all computerised data and physical files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria regardless of the physical location of the filing system.

Data from member/registered organisations will be renewed annually on renewal and data from Non-Member Organisations will be reviewed every three years.

Personal Data

'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A sub-set of personal data is known as 'special category personal data'.

This special category data is information that relates to:

- race or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health;
- an individual's sex life or sexual orientation;
- genetic or biometric data for the purpose of uniquely identifying a natural person.

The Group do collect and hold personal data. The Group may hold special category data for the Group staff members.

Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

The Data Protection Principles

The seven data protection principles as laid down in the GDPR are followed at all times:

1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes; (purpose limitation)
3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed; (data minimisation)
4. personal data shall be accurate and, where necessary, kept up to date;
5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes; (storage limitation)
6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing or access and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. (integrity and confidentiality).
7. The accountability principle requires the Group to take responsibility for what the personal data is used for and compliance with the other principles.

In addition to this, the Group is committed to ensuring that at all times the company is complying with GDPR and anyone dealing with personal data shall be mindful of the individual's rights. This means that the Group will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- be responsible for checking the quality and accuracy of the information;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Records Retention Policy;
- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests;
- report any breaches of the GDPR in accordance with our documented internal procedure.

Consent

Unless it is necessary and only for a reason allowable in the UK GDPR, consent must be obtained from a data subject in order to collect and process their data.

Although the Group do not process the data of minors, in the event that it is required to do so, personal data relating to children below the age of 13 requires parental consent to be obtained beforehand. Transparent information about our usage of minor's personal data must be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

Lawful Basis

The lawful basis for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever we process personal data:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's

personal data which overrides those legitimate interests. More details of this are given in the Privacy Notice.

Disclosure of Personal Data

The following list includes the most usual reasons that the Group will authorise disclosure of personal data to a third party:

- to give a confidential reference relating to a current or former employee, consultant or volunteer;
- for the prevention or detection of crime;
- for the assessment of any tax or duty;
- where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract)
- for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- for the purpose of obtaining legal advice;
- for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- for the purposes of raising invoices for membership and supporting ECTs inductions, seminars, conferences, events, publications and managing and recording the induction processes for ECTs.
- for the purposes of distributing our publications
- for the purposes of the workings of our CRM (Customer Relationship Management) system and websites
- for the purpose of paying employees and paying into their pensions
- to pay consultants and contractors

The Group may receive requests from third parties (i.e. those other than the data subject, the Group or individual entities and its employees) to disclose personal data it holds about individuals. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosure applies, or where disclosure is necessary for the legitimate interests of the third party concerned or the Group.

All requests for the disclosure of personal data must be sent to dpo@cstuk.org.uk or dpo@nta.org.uk, where it will be reviewed and decided whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.

International Transfer of Personal Data

The Group will only transfer personal data outside of the UK or EEA in exceptional circumstances.

In the event that the group is required to transfer data outside the UK EEA, or the third country is not deemed adequate, an International Data Transfer Agreement (IDTA) must be undertaken, for further information please refer to the adequacy section on the ICO website. Then we will ensure that an

appropriate UK GDPR approved IDTA is in any agreement with processors (and their sub-processors) as part of a due diligence process.

In the event that the Group is relying on IDTA's to transfer personal data to a third country, then we will conduct a Transfer Risk Assessment (TRA) to ensure that the third country has suitability in maintaining the privacy of our exported data.

The NTA Entity does have some registered International Schools and therefore reference to the ICO website is imperative prior to sending any information to ensure the adequacy of the location.

Here is a link to the current IDTA template on the ICO website:

https://ico.org.uk/media/for-organisations/documents/4019536/idta.docx

Please contact dpo@cstuk.org.uk or dpo@nta.org.uk in order to undertake the Transfer Risk Assessment process.

Security of Personal Data

The Group will take reasonable steps to ensure that access to any personal data will only be authorised to members of staff, consultants, contractors, volunteers etc to enable them to carry out their duties. The Group have issued this Policy, supporting documentation and annual training to all staff, consultants, contractors, volunteers etc to ensure they are aware of their individual duties under the GDPR and the Group's responsibilities. The Group will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

Subject Access Requests

A Subject Access Request (SAR) is a request made by or on behalf of an individual for the information which they are entitled to ask for under Article 15 of the UK GDPR.

These consist of:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Subject access requests will be processed free of charge unless there is repeated or excessive requests in which case a nominal fee will be charged to the subject per request. The Group have an internal procedure that will be followed for all SAR requests.

All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

All requests received must be sent to dpo@cstuk.org.uk or dpo@nta.org.uk as soon as possible but no later than 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of initial receipt by the Group. These requests could be by any form of communication, including over the telephone. In these circumstances it is important to obtain a telephone number and email address for communication purposes with the data subject, as the Group may need to ask for any further information or clarification on the request. Where possible the individual should be asked to confirm the request in writing via email.

Any individual may appoint another person to request access to their records. In such circumstances the Group must have written evidence that the individual has authorised the person to make the application and must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

All files must be reviewed by the Data Protection Representative before any disclosure takes place. Access will not be granted before this review has taken place.

Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

In responding to a subject access request where personal data is requested to be provided to a subject, the Group will always provide the personal data in a secure electronic format including but not limited to the following file formats:

- CSV
- Word
- Excel
- PDF
- MSG
- ZIP
- JPG

All digital information will be provided to the subject in a compressed ZIP file format which will be encrypted, and password protected. The ZIP file will be electronically transmitted to the subject and the password will be communicated to the subject via alternative means such as verbally communicated over the telephone or via SMS message for example.

Personal data will only be provided to the subject in paper format if explicitly requested.

Complaints Handling

All complaints regarding data protection should be addressed in writing to dpo@cstuk.org.uk or dpo@nta.org.uk and will be acknowledged no later than two business days following receipt of the complaint.

If you are not satisfied with any response from us, then you may contact the Information Commissioner's Office at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

https://ico.org.uk/global/contact-us/email/

Breach of any Requirement of the GDPR

Any and all breaches of the DPA, including a breach of any of the data protection principles shall be reported as soon as it is discovered by staff of the Group, to dpo@cstuk.org.uk or dpo@nta.org.uk.

Once notified, an investigator shall assess:

- the extent of the breach;
- the risks to the data subjects as a consequence of the breach;
- any security measures in place that will protect the information;
- any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Investigator concludes that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Group, unless a delay can be justified.

The Information Commissioner shall be told:

- details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- the contact point for any enquiries (which shall usually be the Data Protection Representative via dpo@cstuk.org.uk or dpo@nta.org.uk);
- the likely consequences of the breach;
- measures proposed or already taken to address the breach.

If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the investigator shall notify data subjects of the breach without undue delay unless the data would be

unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- the nature of the breach;
- who to contact with any questions;
- measures taken to mitigate any risks.

The investigator shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Board and a decision made about implementation of those recommendations.

Compliance

Exceptions to this policy must be approved by the Chief Operating Officer in writing.

All breaches of this policy, actual or suspected must be reported to your line manager initially. In certain cases, the incident may be raised with the IT department and the Information Security Team who will ensure it is investigated. Breaches of this policy may be considered as gross misconduct, and in certain cases lead to termination of employment and/or legal action/prosecution.

APPENDIX 1.0

Table containing category of individuals and type of processes carried out.

Category of Individual	Type of processes carried out
Staff Members	For employment, pension and PAYE obligations For safeguarding obligations
Trustees/Directors	For legal obligations at Companies House and the Charities Commission For legal obligations with some of our suppliers For the payment of expenses For contact regarding meetings and charity accountability
Members/ Service Users	For contact in order to carry out the benefits for Members and our obligations to Members as part of their Membership. For contact in order to manage and record the induction process of ECTs.
Prospective Members/Service Users	Following contact with the Group, to share the benefits of Membership/registration, enable bookings on events and to deal with any questions or queries.
Suppliers	To allow contact and payment of invoices For contact regarding Due Diligence requirements
Consultants/Contractors	To ensure that consultants are compliant with the Group's legal and contractual obligations.