Data Protection Policy

We are currently undergoing our Annual Audit with Risk Evolves which involves a full assessment of our policies, procedures and guidelines.

Our Assessment was delayed due to COVID-19.

We remain fully compliant and our Consultants RiskEvolves are happy to respond to any query regarding or GDPR practices, we will not be updating any dates on our documents until we have finished our annual assessment and received verification from RiskEvolves

Review Date: 11/12/2020
Next Review Date: December 2021
Signed: *Changing Education Group*

Contents

1. Aims

Changing Education Group aims to ensure that all personal data collected about staff, pupils, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This policy applies to all personal data, regardless of whether it is in paper or electronic format collected about staff.

For details of processing related to pupils, parents, visitors and others, please see our Privacy Policy, copy of which can be found on the company website : https://changingeducation.co.uk

2. Legislation and Guidance

This policy meets the requirements of the EU GDPR and the UK Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR and the Data Protection Act 2018 and the ICO's code of practice for subject access requests.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

	• Health - physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

The Changing Education Group are registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required. Our registration number is **ZA091427.**

5. Roles and Responsibilities

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

5.1 The Managing Directors

The Managing Directors have overall responsibility for ensuring that each of our organisations comply with all relevant data protection obligations.

5.2 Data Officer

The Data Officer is responsible for overseeing the implementation of this policy and monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

They will update the Board of Directors and, where relevant, report to the board their advice and recommendations on data protection issues.

Our Data Officer is Stephen Hackney and is contactable via 01625 827309

5.3 All Staff

How we manage data on behalf of our staff and customers is a critical responsibility for all members of staff at Changing Education, regardless of whether they are permanent, temporary, contractors or suppliers. All staff are responsible for:

- processing any data sent by education providers in accordance with this policy
- Contacting the Data Officer in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this 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

We all have a responsibility to look after the data of all staff within the organisation.

6. Data Protection Principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

7. Collecting Personal Data

7.1 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process data where it is necessary for them to carry out their contractual roles. This will be done in accordance with the Group's Information Security and Privacy Policy and any data processing agreements that we have in place with our Clients.

7.2 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Group can fulfil a contract with either an individual (for example, a member of staff), or an organisation (for example, a school, college or supplier) has asked us to take specific steps before entering into a contract
- The data needs to be processed so that we can comply with a legal obligation (for example, right to work checks, or meeting the requirements of HMRC)
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life or for safe guarding purposes
- The data needs to be processed for the legitimate interests of the Group or a third party (provided the individual's rights and freedoms are not overridden). Some examples where an organisation may have a legitimate interest are some limited instances of marketing, or potentially to prevent fraud (eg. credit checks).
- The individual has freely given clear consent

8. The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

8.1 Examples of data that we collect about you :

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.

- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your health, including any medical condition, health and sickness records, including:
- where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
- details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
- where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Information about criminal convictions and offences which is used for DBS checking and vetting.

8.2 How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

9. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- We need to liaise with other agencies (eg. DBS). Where appropriate we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils - for example, our HR Partner, our accountants for payroll processing. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our staff. Where possible, we will seek your permission before doing so, however if the situation is potentially life threatening and you are unable to provide consent, our Data Officer will provide this information.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10. Subject Access Requests

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Group 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 can be submitted verbally or in writing, either by telephone call, letter, email or fax to the Data Officer. They should include:

- Name of individual

- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must **immediately** forward it to the Data Officer.

10.2 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 a child or another individual
- Would reveal that a 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.

10.3 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 (see section 8), individuals also have the right to:

- Withdraw their consent to processing at any time, however this is only relevant when consent was the original lawful basis for having processed the data in the first place.
- 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 Data Officer. If staff receive such a request, they must immediately forward it to the Data Officer.

11. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within **15 days** of receipt of a written request. However, Changing Education Group are defined as Data Processors. All requests must be sent to the contact at the School or College (ie the Data Controller). If you have any doubts or queries on this process, then please contact the Data Officer, Stephen Hackney as soon as possible.

12. Photographs and Videos

As part of our Group's activities, we may take photographs and record images of Individuals.

We will obtain written consent for photographs and videos to be taken of any person for communication, marketing and promotional materials. Inclusion in all photographs used for marketing and promotional purposes is purely voluntary and there will be no detrimental impact on an individual should you chose not to be involved.

Uses may include:
- Pictures within the Group's Newsletter
- Online on our Group website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further however you should be aware that once an image is posted on social media, we cannot guarantee the possibility of deleting it.

When using photographs and videos in this way we will not accompany them with any other personal information about a child.

Whilst there is no current requirement for the use of photographs on id or security

passes, if these are required at a future date then this will be communicated to you.

13. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified Data Officer, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the group's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the Data Officer will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training all members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Data Officer and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Retention of Records

We have a comprehensive register (GDPR Process Mapping) of the type of data that we store and how long we store this information for. Please get in contact if you require further information.

15. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. At Changing Education, we have invested in the IASME scheme, which includes the UK Government's Cyber Essentials scheme and is aligned to the internal information security standard, ISO27001.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on desks, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Further information on how we secure information is held in our Information Security and Privacy Policy and the HR Handbook.

16. Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

17. Personal data breaches

The Group will make all reasonable endeavors to ensure that there are no personal data breaches. However, we are mindful that mistakes can and do happen. If you are aware of any incident, or a 'near miss' where the organisation has the opportunity to improve, then please contact the Data Officer asap.

When appropriate, we will follow our Data Breach Procedure and report the data breach to the ICO within **72 hours**. Such breaches may include, but are not limited to:

- The theft of any portable device.
- The theft or loss of any data.
- Ransomware on our computer system
- The loss of any paper records.

In the event that personal information relating to staff is lost, you will be notified with 72

hours of any loss.

Like the theft of any asset from a business, we have a zero tolerance approach should we discover the malicious loss or theft of data.

18. Training

All Directors and all staff 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 group's processes make it necessary.

19. Monitoring Arrangements

The Data Officer is responsible for monitoring and reviewing this policy.

20. Links with other policies

This data protection policy is linked to our:

- Group Privacy Notice.
- CONNECT Data Processing agreement.
- HR Handbook
- Data Breach Procedure
- Incident Management Procedure