EqualiTeach Data Protection and Cyber Security Policy

Policy accepted on: 10/10/2022

Policy review due on: 10/10/2025

Purpose

EqualiTeach's Data Protection and Cyber Security Policy outlines the following information:

- What data we keep and why
- Key precautions to keep data protected
- How data is stored, handled and destroyed and who is responsible for these processes
- What to do if an individual asks to see their data and when a Subject Access Request will be denied
- Under what circumstances EqualiTeach will disclose data and to whom
- How EqualiTeach ensures cyber security
- Procedure if EqualiTeach experiences a data breach and/or security incident

All staff must be familiar with this document.

Data Processing

EqualiTeach will ensure that it has at least one of the necessary valid reasons for processing the data it is holding:

- The individual whom the personal data is about has consented to the processing;

- The processing is necessary: in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract;

- The processing is necessary because of a legal obligation that applies to EqualiTeach;

- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department;

- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions;

- The processing is in accordance with the "legitimate interests" condition

Personal Data and Sensitive Personal Data

For data to be classified as personal data, it will:

1. Be data (so not unrecorded conversations with service users, donors or customers);
2. Be personal. Data is personal if it is concerned with identifiable, living individuals. It does not matter whether this data was processed automatically, electronically or manually. Personal data includes IP addresses, internet cookies and biometrics, such as DNA and fingerprints.

For data to be classified as sensitive personal data, it must fall into the following categories:

1. The racial or ethnic origin of the subject;
2. The subject's political opinions;
3. The subject's religious beliefs or beliefs of a similar nature;
4. Whether the subject is a member of a trade union;
5. Information on the subject's physical or mental health condition;
6. Information on the subject's sexual orientation
7. The commission or alleged commission of an offence by the data subject;
8. Information relating to the commission or alleged commission of an offence by the data subject.

Article 5 of the GDPR contains the principles and requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

EqualiTeach is committed to upholding the principles and requirements under Article 5 of the GDPR.

EqualiTeach Staff

Employee Recruitment

The following data is collected from employees on their recruitment:

Full name, date of birth, National Insurance number, address, telephone numbers, email addresses, next of kin name and contact details, medical conditions, bank name, bank address, sort code, account number, photocopy of two forms of identification, photocopy of qualification and examination certificates, and business car insurance details.

This data is collected in order to fulfil the requirements of the contract with the individual and to ensure that EqualiTeach is compliant with its legal obligations when recruiting. EqualiTeach communicates the reasons why the following data is collated with new and existing employees via a Privacy Notice given to staff on receipt of a conditional job offer.

This information is stored in online folders accessible only to the recruitment team at EqualiTeach on encrypted laptops. Online personal information should not be

accessed on personal computers, personal tablets or other devices and phones. Hard copies are stored in box files in the lockable cupboard in the executive directors' office. The executive directors of EqualiTeach are responsible for ensuring that the cupboard is locked at all times and is only accessed by members of senior management.

Emails containing personal data are permanently deleted from staff inboxes once it no longer serves a purpose/has been transferred to the relevant files. Emails containing personal data should never be forwarded to people not involved with recruitment or human resources, external clients or to personal email addresses.

Employee Financial Data

Any correspondence from HMRC or other bodies providing financial data for employees is stored in box files in the lockable cupboard in the executive directors' office and will be shared only with the relevant member of staff. Financial data should not be exchanged via email.

Electronic employee financial data is stored in a SharePoint account accessible only to the executive directors, EqualiTeach's accountant and the Operations Manager.

Financial data contained in fundraising applications is saved in a password protected SharePoint folder and is accessible only to the fundraising team.

Payroll information is held in online folders, to which only the executive directors and EqualiTeach's accountant have access. This is password protected.

Payroll is controlled by EqualiTeach's accountant. Only executive directors and the Head of Operations are permitted to access payroll information.

Pension information is stored electronically on the password protected Wren Sterling Master Trust online portal.

DBS Certificate Information

DBS information is stored online at UKCRBS.com. Only the executive directors will have access to DBS information. Hard copies are stored in box files in the lockable cupboard in the executive director's office.

DBS Numbers and Dates of Issue for all staff members are accessible on online folders to all staff members for the purposes of providing these to schools, in accordance with EqualiTeach's DBS Policy and written Statement of Assurance. These documents are password protected.

Emails containing DBS information should be permanently deleted from staff inboxes once their existence no longer serves a purpose. DBS information should not be accessed on personal computers, personal iPads or other devices or phones.

Probationary Review, Supervision and Appraisal Minutes

Staff members have individual online folders for their probationary review, supervision and appraisal minutes, accessible only to their line manager and the relevant staff member.

Emails containing minutes of personal meetings, such as supervisions, appraisal, performance management or disciplinary meetings, should be permanently deleted from staff inboxes once their existence no longer serves a purpose. Minutes of personal meetings should not be accessed on personal computers, personal iPads or other devices or phones.

Employee Use of Organisation Computers

All work computers are password protected and encrypted. Organisation computer systems are to be used only for the business of the organisation and not to be used for personal activities. Staff members must not purposely engage in activity with the intent to: harass others, degrade the performance of the system; divert system resources to their own use; or gain access to organisation systems for which they do not have authorisation. Staff members must not attach unauthorised devices to their computers or workstations, unless they have received specific authorisation from an executive director. Staff members must not download unauthorised software from the internet onto their computers or workstations.

When transporting laptops outside of the office, staff members must ensure that appropriate care is taken to avoid theft or loss of the laptop. Laptops must be kept in a secured building overnight; laptops must not be stored in a car overnight or taken with the staff member to any non-work-related engagement.

Staff members are required to report any weaknesses in the organisation's computer security, any incidents of misuse or violation of this policy to their line manager.

Anti-virus software will be installed on all work computers and must be kept up-to-date by each staff member. No other anti-virus or anti-malware software should be installed without permission from the Head of Operations.

Staff members should change their computer and email password at least every six months to reduce the risk of a security incident and/or data breach. All passwords should contain at least one capital letter, one number and one punctuation mark.

Use of the Internet

The internet is a business tool for the organisation. EqualiTeach will provide internet access to employees and contractors who have a business need for this access.

The internet is to be used for business-related purposes such as: communicating via email with customers, suppliers and business partners, obtaining information useful for achieving the organisation's aims.

The internet may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature or any other purpose which is illegal or for personal gain.

Passwords gaining access to the organisation's data are changed as soon as possible if an employee is suspended, an employee's contract is terminated, or an employee otherwise leaves the employment of the organisation.

Online purchases must be made using an official EqualiTeach account with each provider and by a member of senior management and/or the Operations team. If a member of staff who is not a member of senior management or the Operations team wishes to purchase an item, this must be referred to the Programme Support Officer, who will purchase the item on their behalf and in line with organisational budgets.

Only members of the senior management and/or the Operations team have access to EqualiTeach's hosting provider account, the EqualiTeach website account and the Equalities Award website account.

The security track-record of hosting providers is of the upmost importance and the EqualiTeach hosting provider is chosen with this at the forefront of decisions made.

Employee Use of Personal Computers, iPads and Phones

Employees are not permitted to use personal computers and/or iPads for business purposes except in exceptional circumstances. In these cases, permission to use a personal computer must be requested from their line manager in writing. Where permission is granted, employees should not download SharePoint onto their personal desktop or save passwords to access online business accounts in browsers.

Employees are permitted to use personal phones for business purposes. Phones should be password protected. Employees are permitted to download software, such as Outlook, on their personal phones but these must be password protected.

Employees are permitted to access software such as SharePoint accounts on school computers, for example, to download and use PowerPoints where use of USBs is prohibited. SharePoint accounts should never be downloaded on school computer desktops. Username and passwords to access software on school computers should not be saved in browsers, accounts should be logged out of and all accessed documents should be closed at the end of use.

EqualiTeach Advisory Board Member Data

Any personal or sensitive data of Advisory Board members will be kept electronically in password protected folders and in hard copy in a box file in the lockable cupboard accessible only to the executive directors.

Changes to Personal Data

Staff members should ensure that their line manager is made aware of any changes to their personal data. Records will then be updated accordingly, and out-of-date information will be permanently deleted immediately.

Protocols for Outgoing Employees

Outgoing employees must return their keys (two to the office door and one to the building door) to a member of the Operations team on their last day in the office. The outgoing employee must sign that they have returned their keys and the Operations team member must sign that they have received their keys. Spare keys are stored in a lockable cabinet to which only senior management has access.

Outgoing employees must permanently delete any personal data from their laptop and all online software. Hard copies must be shredded in the office by the Head of Operations.

If an outgoing employee had access to usernames and passwords to online accounts, these must be changed on their leaving.

Deleting the Personal Data of Previous Employees

All personal data of employees are deleted within six months of the employee's leaving date. Electronic copies of personal data are permanently deleted from laptops and all online software. Hard copies are shredded in a cross-cut shredder. Shredded material must be disposed of in the organisation's recycling bin.

EqualiTeach Job Candidates

Candidate's Personal Data

Job application forms request the following personal data: full name, address, telephone number, email address, right to work in the UK, and confirmation of convictions, cautions, reprimands and warnings. Job application forms are stored electronically in a SharePoint folder accessible only to the recruitment team. Hard copies are stored in a box file in a lockable cupboard.

Shortlisted application forms are shared via SharePoint with members of the Advisory Board, who are subject to this Data Protection Policy and the Code of Conduct for Advisory Board members. Any printed versions of application forms

should have personal data removed. No identifying information must be shared with staff members not involved in recruitment or publicly.

Deleting Data of Unsuccessful Candidates

The personal data of unsuccessful candidates is destroyed after a maximum of six months. Electronic data is permanently deleted. Hard copies are shredded.

Collection of Candidates' Monitoring Information

Sensitive personal data is collected from candidates anonymously using a monitoring form separate to the job application form. It is not mandatory for candidates to complete a monitoring form. The monitoring form is separated from the job application as soon as they are received. Paper copies of monitoring forms are collected in a box file in a lockable cupboard. Electronic monitoring forms are saved in a SharePoint folder, to which only the recruitment team have access. Monitoring data is collated, analysed and retained indefinitely in order to ensure that EqualiTeach are attracting as wider pool of talent as possible. This is in the legitimate interests of the organisation. Once monitoring data has been collated, electronic monitoring forms are deleted and paper monitoring forms are destroyed using a cross-cut shredder.

Subject Access Requests

Individuals have the right to request, either via email or writing, the following:

- Confirmation that their data is being processed
- Access to their personal data, and
- Other supplementary information

In most circumstances, EqualiTeach will provide the information requested free of charge. EqualiTeach will charge a fee based on the administrative cost of providing the information when a request is manifestly unfounded, excessive or repetitive.

Information will be provided without delay and within a month. Where requests are complex or numerous, EqualiTeach will extend the deadline to three months. However, EqualiTeach will still respond to the request within a month to explain why the extension is necessary.

For more information, please see EqualiTeach's Subject Access Request Procedure.

EqualiTeach Client and Potential Client Data

Data held about EqualiTeach clients can include, but is not limited to:

- Name of contact and name of client organisation
- Address of client organisation
- Email address and phone number(s)
- Financial details, such as name of bank, sort code and account number

This information is used only for purpose of providing clients with a service and is not passed onto any third parties.

Data is saved in online password protected client relationship management software and in spreadsheets used for monitoring, promotions and marketing, to which all staff members who service clients have access. Hard copies of customer data will be destroyed using a cross-cut shredder, which will be emptied into EqualiTeach's recycling bin by the Head of Operations.

Data is saved online in online accounting software accessible only to the senior management team and business development team. Downloaded invoices are saved in a invitation-only SharePoint folder and paid invoices are only accessible to the senior management team in a separate SharePoint folder.

Only Equalities Award team members have access to the Equalities Award backend system. This is password protected. No customer data should be downloaded from the Equalities Award backend.

Emails containing client data are permanently deleted from staff inboxes once they no longer serve a purpose/the data has been transferred to the relevant files. Emails containing personal data should never be forwarded to other staff members not involved with that client's service, other external clients or to personal email addresses.

Email addresses of clients saved on Outlook are accessible only on password protected and encrypted computers and mobile devices.

At the end of a project, data will be kept for 12 months and then permanently deleted from all software.

Requests for the deletion of client data

GDPR gives individuals the right to ask for their data to be deleted and EqualiTeach has an obligation to do so, except in the following circumstances:

- The personal data is needed to exercise the right of freedom of expression.
- There is a legal obligation to keep that data.
- For reasons of public interest (for example, public health, scientific, statistical or historical research purposes).

Data collected from minors must be deleted.

EqualiTeach will take reasonable steps to inform other websites that a particular individual has requested the erasure of their personal data.

Data can be kept if it has undergone an appropriate process of anonymisation.

Newsletter Sign up Data

When clients and potential clients sign up to EqualiTeach's quarterly newsletter, the following data is collected:

- Name of contact
- Email address of contact
- Name of contact's school/organisation

Name of contact and email address of contact is saved in Excel spreadsheets in a password protected SharePoint folder, accessible only to the senior management team and the member of staff responsible to data entry and uploading. Excel spreadsheets are deleted once they no longer serve a purpose. The data is uploaded to Mailjet software, which is used to automatically send out newsletters.

Mailjet software is password protected.

Hard copies of data for the newsletter is kept in box files in the office.

For information about Equalities Award client data, please see the Equalities Award Privacy Policy.

Password Storage

All passwords are stored in a password protected spreadsheet accessible only to the executive directors. Some of these passwords, for example for utilities and IT accounts, are saved in a password protected spreadsheet accessible only to the executive directors and the Operations team.

Website Cookies

EqualiTeach's websites (the main website, the Equalities Award website, the e-learning website and the Empowered website) use cookies. This information can be used to track clients' sessions on each site. Cookies may also be used to customise websites for individual clients. If clients use a common internet web browser, they can set up their browser to either let them know when they receive a cookie or to deny cookie access to their computer. We work with Google Analytics who may also, through cookies, track your experience with our websites including where clients came from, what clients did whilst using the websites and where clients went after landing on webpages.

Data Breaches

The Information Commissioner's Office describes a personal data breach as "a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data."

All data breaches should be reported immediately to the Head of Operations, or failing that, another member of senior management. Those involved in breaches of personal data may be subject to investigation by the executive directors using the EqualiTeach Disciplinary Procedure.

If a breach is likely to result in a risk to the rights and freedoms of individuals, then the breach must be reported to the Information Commissioner's Office within 72 hours. If a breach is likely to result in a high risk (e.g. criminal activity such as fraud or published in the public domain) to the rights and freedoms of individuals, the Head of Operations will notify those concerned without undue delay. Breaches are reported at www.ico.org.uk/for-organisations/ report-a-breach/

Security Incident Handling Procedure

A security incident is any irregular or adverse event that threatens the security, integrity or availability of information on any part of the organisation's network. For example,

- Illegal access of an organisation computer system
- Damage to an organisation computer system or network caused by illegal access
- Malicious use of system resources to launch an attack against other computers outside of the organisation network

Employees who believe their computer system has been subjected to a security incident, or have otherwise been improperly accessed or used, should report the situation to the Head of Operations immediately or, failing that, another member of senior management. The employee should not turn off the computer or delete suspicious files but instead hand over the computer to the Head of Operations who will investigate and remedy the issue.

Breaches of the Policy

EqualiTeach will support employees who become aware of and are willing to report breaches of this policy or who genuinely believe that a breach is occurring, has

occurred or is likely to occur within the business. Employees should raise the issue internally with their line manager.

Employees who fail to comply with the guidance detailed in this policy could be subject, following full investigation, to disciplinary action up to and including dismissal.
