EmpowerEd
Unlocking potential, building futures

EmpowerEd Data Protection Policy

Date of last review: 10/08/2023

Date of Next Review: 10/08/2024

EmpowerEd Data Protection Policy Statement of Intent

EmpowerEd is required to keep and process certain information about its staff members, contractors (including tutors) and tutees and other third parties in accordance with its legal obligations under the EU General Data Protection Regulation (GDPR).

EmpowerEd may, from time to time, be required to share personal information about its staff or pupils with regulatory and potentially children's services. This policy is in place to ensure all staff and trustees are aware of their responsibilities and outlines how EmpowerEd complies with the following core principles of the EU GDPR. Organisational methods for keeping data secure are imperative, and EmpowerEd believes that it is good practice to keep clear practical policies, backed up by written procedures.

1. This policy has due regard to legislation, including, but not limited to the following: The General Data Protection Regulation (GDPR), The Freedom of Information Act 2000, The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016), The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
2. This policy will be implemented in conjunction with the following documents: EmpowerEd Handbook, EmpowerEd Child Protection and Safeguarding Policy, EmpowerEd Privacy Notice.

3. Sources For the purposes of EmpowerEd.s' business, personal or sensitive information may derive from various sources, such as:
• Employees (and close relations, e.g. emergency and next of kin contacts).
• Ex-employees.
• Potential and prospective employees.
• Referees.
• Client records.
• Targeted school individuals (marketing).
• School pupils.
• Trustees/patrons.
• Grant funders/donors/professional partners.
• Tutors.
• Tutor alumni.

4. Applicable data

4.1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

4.2. Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

5. EmpowerEd will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the above principles set out in the GDPR.

6. EmpowerEd will provide comprehensive, clear and transparent privacy policies.

7. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

8. EmpowerEd will implement measures that meet the principles of data protection by design and data protection by default, such as:

• Data minimisation.
• Pseudonymising.
• Transparency.
• Allowing individuals to monitor processing.
• Continuously creating and improving security features.

9. Under the GDPR, data will be lawfully processed under the following conditions:

• The consent of the data subject has been obtained.
• Processing is necessary for: Compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, for the performance of a contract with the data subject or to take steps to enter into a contract, protecting the vital interests of a data subject or another person, for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by EmpowerEd. in the performance of its tasks.)

10. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

11. Where consent is given, a record will be kept documenting how and when consent was given.

12. EmpowerEd ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

13. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

14. Consent can be withdrawn by the individual at any time.

15. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

16. Legitimate Interests EmpowerEd. relies on the legitimate interest basis for some of their uses of constituents' personal data, like performing analytics. Using legitimate interest requires that we:

• Conduct a balancing test.
• Tell constituents that you're relying on legitimate interests;
• Allow constituents to opt out of the processing.

17. PECR/ePrivacy Unsolicited marketing by e-mail, fax, text, or phone, EmpowerEd. complies with both GDPR and the UK's Privacy and Electronic Communication Regulations ("PECR"). Under PECR, to send direct marketing to 'natural persons', EmpowerEd.:

• Will obtain consent where necessary, or
• Marketing to an existing customer in the context of the sale of a product or service. This is referred to as the "soft opt-in." EmpowerEd. sells services so they can take advantage of the 'soft option' only with the appropriate initial consent.

18. The lawful basis for your processing data can also affect which rights are available to individuals. For example: Right to erasure Right to portability Consent ✓ ✓ Contract ✓ ✓ Legal obligation X X Vital interests ✓ X Public task X X Legitimate interests ✓ X * but right to withdraw consent

19. Automated decision making and profiling

20. Individuals have the right not to be subject to a decision when:

• It is based on automated processing, e.g. profiling.
• It produces a legal effect or a similarly significant effect on the individual.

21. EmpowerEd. will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

22. When automatically processing personal data for profiling purposes, EmpowerEd. will ensure that the appropriate safeguards are in place, including:

• Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
• Using appropriate mathematical or statistical procedures.
• Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
• Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:
• EmpowerEd. has the explicit consent of the individual.
• The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

23. Confidential paper records will not be left unattended or in clear view anywhere with general access.

24. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

25. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

26. Memory sticks will not be used to hold personal information unless they are password protected and fully encrypted.

27. All electronic devices are password-protected to protect the information on the device in case of theft.

28. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.

29. Emails containing sensitive or confidential information are password protected if there are unsecure servers between the sender and the recipient.

30. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from EmpowerEd. premises accepts full responsibility for the security of the data.

31. Before sharing data, all staff members will ensure:

• They are permitted to share it.
• That adequate security is in place to protect it.
• Who will receive the data has been outlined in a privacy notice.

32. The physical security of EmpowerEd. buildings and storage systems, and access to them, is reviewed on a yearly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

33. EmpowerEd. takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

34. The DPO is responsible for continuity and recovery measures that are in place to ensure the security of protected data.

35. EmpowerEd. publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

• Policies and procedures.
• Annual reports.

36. EmpowerEd. will not publish any personal information, including photos, on its website without the permission of the affected individual.

37. When uploading information to EmpowerEd. website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

38. EmpowerEd. understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

39. EmpowerEd. will always indicate its intentions for taking photographs of pupils and tutors and will retrieve permission before publishing them.

40. If EmpowerEd. wishes to use images/video footage of pupils in a publication, such as EmpowerEd. website, written permission will be sought for the particular usage from the parent of the pupil (through the centre.)

41. Data will not be kept for longer than is necessary and in-line with relevant legislation. All data retained will be reviewed annually.

42. Unrequired data will be deleted as soon as practicable.

43. Some records relating to employees of EmpowerEd. may be kept for an extended period for legal reasons, but also to enable the provision of references.

44. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

45. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

46. Data provided by the DBS will never be duplicated.

47. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

EmpowerEd. Employees' Responsibility:

48. Compliance with this Policy is the responsibility of every employee of EmpowerEd. (including temporary employees and consultants), and any person who

acts on behalf of EmpowerEd. and any person who has responsibilities for the collection, access or processing of personal data.

49. Employees must understand what is meant by personal and sensitive data, and know how to handle such data.

50. Each employee of EmpowerEd. is required to:-

• Read and understand this Data Protection Policy;
• Adhere and abide to this Data Protection Policy;
• Share best practice on data protection issues;
• Attend training sessions and read updates as directed;
• Read and adhere to any changes or updates to this Data Protection Policy when notified of such changes or updates.
• Report concerns relating to data protection to EmpowerEd. Data Protection Officer, Mandy Gallego. Contractors, Data Processors, Consultants, Agents and other Third Parties

51. All contractors, Data Processors, agents, consultants, partners, sub-contractors and other third parties acting on behalf of EmpowerEd., including tutors, must:

• Ensure that they and all employees who have access to personal data held or processed for or on behalf of EmpowerEd., are aware of this policy and are fully aware of their duties and responsibilities under the GDPR Act
• Any breach of any provision of GDPR will be deemed as being a breach of any contract between EmpowerEd. and that individual, company, partner, organisation or firm
• Allow data protection audits by EmpowerEd. of personal data held on its behalf (if requested)
• Indemnify EmpowerEd. against any prosecution, claims proceedings, actions or payments of compensation or damages, without limitation.

Clear Desk Policy

EmpowerEd. operates a clear desk policy in the office. Employees must follow the guidelines below:

• All personal information should be locked away when desks are unattended, especially overnight. Particularly sensitive information may need to be kept in a fire-retardant cabinet or safe.

• Where the volume of paperwork prevents it from being locked away, it should still be kept tidy and out of the way as far as possible. Files, boxes and crates blocking corridors or fire exits create a safety hazard.
• All papers should be collected immediately from printers and faxes.
• Particular care should be taken of documents taken outside the office.
• GDPR data protection regulations apply to data about individuals which is created, stored, transmitted or disclosed as a paper record.
• Computers should be locked if desks are left unattended for any period of time. Further, a full log out should be completed prior to leaving the office.

52. A review will be completed on an annual basis to provide reasonable assurance that the policy and procedures are working effectively and to enable risk areas to be identified and addressed.

Policy review

This policy is reviewed annually by the DPO. The next scheduled review date for this policy is August 2024.

Any concerns or questions should be directed to the DPO:
Chris Vasquez
chris@empowered-education.co.uk