Mentoring Women in Business Data Protection

Introduction

We want participants of the Mentoring Women in Business programme to know your rights and responsibilities when it comes to your personal data. To learn more about how the Mentoring Team handles the data that we collect from our mentees and mentors, please find our Privacy Policy here. It is also important to recognise that information that gets shared between mentees and mentors during their mentoring sessions does not get overseen or monitored by the Mentoring Team. Participants must therefore follow our Code of Conduct. This states that the mentoring meetings are confidential. This means that it is our participants' responsibility to ensure that personal or sensitive data is not made available to people outside of the mentoring relationship. In doing this, you will play your part in ensuring that the Cherie Blair Foundation for Women meets its obligations under the UK General Data Protection Regulation (UK GDPR). To help our participants securely handle data, we have developed a list of important considerations you should follow.

How to securely handle personal data

There are some simple strategies that participants of the Mentoring Programme can follow to ensure good data practice. Mentees and mentors should:

1. Only write down or otherwise record personal or sensitive data that is relevant and necessary for the mentoring relationship.

2. Delete any data when it is no longer relevant or no longer correct. Participants must also delete all data at the end of the mentoring relationship.

3. Try to ensure that you are not overheard during their mentoring meetings, for example by avoiding taking the call in a coffee shop, your company's cafeteria or on public transport.

4. Make sure that written notes are kept in a personal notebook, folder or other safe place that no other people can access.

5. Ensure that any data they documents stored on a secure device and in a secure place. This includes making sure that the device has up to date anti-virus, malware and security software.

6. Ensure that your device is secured with a strong password that is only known to you. It is also important that the device is turned off or locked when not in use, so no other people can access it.

7. Obtain written consent from your mentoring partner before you share personal data with anyone outside of your mentoring meetings. This includes sharing on social media.

8. Consider encrypting files that include personal data by securing the file with a password. If an encrypted file is shared, it is important that the password is not included in the same email but discussed during a call or send via a different channel (e.g. a text).

9. Talk to your company's IT department to learn more about the security they offer, if you're conducting the mentoring relationship at your place of work or using work equipment.

Support

Mentees and mentors should contact the Mentoring Team if you have any further questions about the data that the Foundation collects or the data that participants handle themselves. The Team can share useful resources or offer personalised advice. It is also important that participants get in touch with us immediately if any personal information does get shared outside of the mentoring relationship (even unintentionally).