MentorNet Data Security

Introduction

This document describes how data security is managed within the MentorNet platform in order to keep sensitive data confidential and in order to restrict access to only authorised users. It also explains how sfG Software and MentorNet fulfil the obligations of the UK Data Protection Act (1998).

General

Put simply, there is no way any person who doesn't have an active MentorNet account can access data in the system. MentorNet accounts are managed by you (or us sometimes if you need help) and so you have full control over who has access to the system and the data. The following describes how we manage this security.

Access to MentorNet Data

The only people who can gain access to MentorNet data are users with a valid MentorNet account (set up within MentorNet), which will include the following:

- Your mentors and mentees
- Your administrators
- sfG staff

Each MentorNet user has a unique account username and password with a strong password enforcement policy. MentorNet users are created and managed by the MentorNet administrator (ie you) and can be disabled by you in order to remove their access.

MentorNet has very strict security which allows you, as the administrator, to define precisely what data mentors and mentees have access to. You can therefore ensure that mentors and mentees see only data relevant to them and have no access to confidential information about others. See later in this document for more details.

Typically your administrators have access to all data within MentorNet, but we can also restrict access to some of the more sensitive data, should you so wish.

Staff within the MentorNet development team require access to the underlying database and therefore have access to MentorNet data. Access and confidentiality of this data is protected as follows:

- All employees of sfG Software require to sign a confidentiality agreement as part of their employment contract
- sfG Software typically does not use contractors for any development work, but in the rare occasion when this does happen, the contractor would have to sign a confidentiality agreement
- Access to the underlying MentorNet database is limited to staff in the development team who require access
- Administrative access to MentorNet is through an administrative login with a strong password enforcement policy.

Departing or suspended users of the system can have their accounts disabled or deleted so that their access is removed. Deleting the account deletes all associated data so you can't recover it; disabling the account 'suspends' the account so that you are able, at a future date, to make the account active again and view all the data. You, as administrator, are able to make this choice. Either way, a deleted or disabled user cannot access the system or any data.

MentorNet Data Security

Data Storage

- All data is stored in secure data centres within Europe (currently the UK, Ireland or the Netherlands). Data centre staff do not have access to the MentorNet data.
- In order to prevent unauthorised access to the system, MentorNet uses forms authentication over a secure (SSL) connection.
- The server platform is Windows Server 2012 R2 running IIS8.5 for websites and Windows Server 2012 R2 and SQL Server 2012 for the database server. The connection to the site is using SSL link, and the servers are PCI compliant.
- Security patches are installed on a monthly schedule and we block remote access with FTP and RDP from the Internet. The Windows 2012 R2 servers use Windows firewall for security.

Data Encryption

MentorNet's password hashing uses SHA512 and it also salts and base64's the password. Our security certificate uses SHA2 (SHA256) as its "Signature Hash Algorithm".

The data at rest in the MentorNet database is encrypted using "Transparent Data Encryption" (TDE). All database backups remain encrypted. Our implementation of TDE uses AES-128 server side encryption to encrypt at both file and SQL object level.

'Acceptable Use Policy' for MentorNet Users

All MentorNet users are forced to read and sign an 'Acceptable Use Policy' before they can get access to the system. This policy is written by you, or we can provide a suggested template for you to amend. This ensures that all users of the system are aware of how their data will be used and what their obligations are.

UK Data Protection Act (1998)

Our Subscription Agreement, which both parties will sign, contains the detail of how we fulfil our obligations under the UK Data Protection Act (DPA).

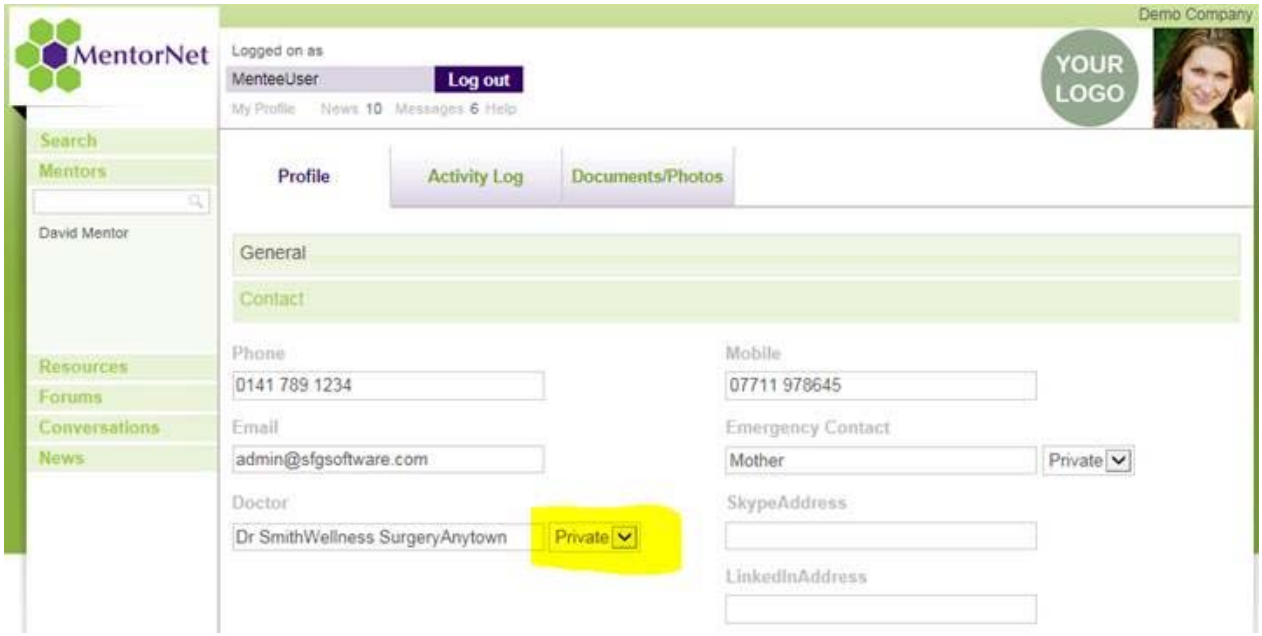
In summary, you will act as Data Controller and sfG Software will act as a Data Processor within the terms of the Data Protection Act 1998. We, as Data Processor, undertake to process data as defined in the DPA by:

a) acting only on the instructions of the Data Controller;
b) performing such actions as are necessary to ensure we have fulfilled, and will continue to fulfil, our responsibilities;
c) complying with any changes in applicable laws. In the event we are unable to do so, we shall forthwith notify you and the you shall be entitled to terminate this agreement, unless the parties have agreed or forthwith agree to take such steps as shall enable us so to comply;
d) storing all MentorNet data only within UK-based data centres;
e) refraining from subcontracting the processing of your data without your consent.

Restricting Access to Personal Information

It is possible to define individual fields in a user's profile as 'private' which means that only the administrator and user can view those details; no other user is able to view them. So, for example, if you have a field that holds the mentee's email address or phone number then that field could be made "private" so that the mentor is unable to view that data for the mentee.

The screenshots below illustrate the point. The first screenshot shows how the profile security settings for a user can be edited to make specific fields private – the highlighted bit shows how the "Doctor" field can be changed between 'public' and 'private' to determine who has access to the data in the field.



The second screenshot shows what this mentee's mentor will see when he views her profile – you can see that the "Doctor" field is not visible.