M22 (2016) Safeguarding Records

Contact Name and Details	Tim Carter, Connexional Safeguarding Adviser cartert@methodistchurch.org.uk
Status of Paper	Final
Action Required	None
Resolution	61/1. The Council receives the report.

Memorial M22 (2016) Systems for recording safeguarding cases

In light of the revised guidance *Safeguarding Records: Joint Practice Guidance for Church of England and The Methodist Church*, the Southend and Leigh (34/10) Circuit Meeting (Present: 43; Voting: unanimous) recommends and requests that the Methodist Church develops a secure connexional online system for safeguarding recording and reporting to ensure consistent and effective compliance with data protection legislation, and good practice. This system could be part of the Methodist online suite.

Reply

The Conference thanks the Southend and Leigh Circuit Meeting for highlighting the importance of storing the required safeguarding information and that this be in a secure and compliant environment.

The revised guidance *Safeguarding Records: Joint Practice Guidance for Church of England and The Methodist Church* should be followed across the Connexion and is available on the Church website at http://www.methodist.org.uk/media/1517149/Safeguarding%20recording%20guidance16%2012%2014.pdf.

The Conference directs the Methodist Council to oversee an investigation of the potential feasibility and cost of a system as described in the memorial and to report back no later than the 2018 Conference.

1. Work undertaken to date has identified the following principles for such a system:

   - The users of this system would be District Safeguarding Officers (DSOs), Professional Supervisors and members of the Connexional Safeguarding Team (CST). Access would also need to be granted to those who need to maintain the website, the hardware and software needed to operate the website and for backup purposes.

   - The online system would allow DSOs to raise new safeguarding cases, as well as view and edit cases within their district. Any case they raise is automatically allocated to them and the CST could allocate additional cases to them.

   - Members of the CST would use the back office application to register DSOs and Professional Supervisors on the site. A password would be provided, which would need to be changed on first access. The site would use two-factor authentication, meaning the user would have to enter an additional randomly generated password along with their username and password.

- Users must use a modern browser, such as Edge, Chrome, Firefox, or Internet Explorer 10 or 11. If an older browser is used, such as Internet Explorer 9 or older, access would be blocked by the system.

- The site would contain a dashboard listing all active cases, along with deadlines and case allocation information. The user's role determines what information is displayed. Users could log in as DSO or Supervisor.

- DSOs would only see cases within their districts. They would be able to add new cases and edit existing cases. Fields would either be editable or read only. Read only fields would display data entered by a member of the CST, or created automatically by the system.

- DSOs would be able to generate reports relevant to the requirements of the role.

- Old cases would not be fully accessible (ie cases created before the system goes live) as there may be sensitive information that was not envisaged to be shared at the time that it was created. An indicator record would display instead with further information only accessible by contacting a member of the CST. These old cases would be manually uploaded by the CST using the back office applications.

- The Professional Supervisor would have access to the Online Safeguarding System. Their access would be restricted to cases where the DSOs they are supervising have been assigned with the provision to assign cases to other professional supervisors when cover is needed ie due to annual leave or sickness. They would also need access to cases where the DSO is the subject of a case. They would be able to generate reports on cases allocated to their DSO, how many cases were dealt with within the deadline and how many missed the deadline. Additional reports still to be decided.

- Due to the sensitive nature of the safeguarding data, support for the system would need to be led by the CST. The Web Applications Team could manage difficulties with logging in and passwords, but queries relating to cases would have to be dealt with by the CST. Further discussion is required on this issue.

2. There are however a number of areas that require further testing:

   - The relationship between Professional Supervisors and DSOs will begin to be implemented from September and therefore a new system will need to be informed by the learning from what is most useful in shared recording.

   - This will include clarification on what reports are required. These could be developed at a later date if required.

   - Clarification is needed on how the information about Safeguarding Contracts is to be presented.

   - Further work is required to define levels of access and deal with conflicts of interest, such as if a DSO is the subject of a safeguarding case. Similarly, if a Professional Supervisor or member of the Safeguarding Committee are subjects.

- Two-Factor Authentication would need to be in line with Methodist Church Security Policy / Remote working guidance.

- This system would of course need to be designed to be compliant with the requirements of GDPR which come into force on 25 May 2018.

- Indicative costs are showing an initial spend of £20k with an additional ongoing cost of £3k pa

- Further work is needed to establish how this would connect with the development of software for accounting use around the Church (M21 2016).

3. Further work will therefore be undertaken to address the concerns raised above and a fully costed plan with any related policy decisions will be brought to the Council by January 2019.

*****RESOLUTION**

61/1. The Council receives the report.