Social Media Policy

1. The Policy

1.1. Social media is an innovative way of engaging people in consultation and participative activities. It can be particularly useful in engaging with those who are not readily engaged using traditional participative tools.

1.2. The Deafness Resource Centre Ltd (henceforth 'DRC') recognises that it needs to embrace social media or it risks failing to engage with an increasingly large segment of the community.

1.3. The DRC will use Social Media tools to engage with the public where it is considered that such tools will provide an effective means of community engagement. However, safeguarding the reputation of the DRC will remain the key consideration in determining how and when Social Media is used.

2. Purpose of this Policy

2.1. Social media presents the DRC with new opportunities to understand, engage and communicate. The potential of social media as a business tool is almost limitless. However if misused, it has the potential to cause considerable damage to the DRC, and those we seek to engage with.

2.2. The most obvious examples of popular social media tools are Facebook, Twitter and YouTube. These facilities, and ones like them, have very rapidly changed the way in which individuals communicate with one another, increasingly overshadowing even e-mail accounts and text messages.

2.3. The purpose of this policy is to ensure that where the DRC uses social media, it does so in a controlled manner that enables us to engage safely and effectively.

2.4. The policy seeks to ensure that the reputation of the DRC is not adversely affected through our use of social media, and that the DRC is not exposed to legal and governance risks that can be very significant.

3. Risks from Inappropriate use of Social Media

3.1. The power of social media carries considerable organisational risk. The ease in which individuals can place information and opinion in a very public domain means that its use has to be appropriately controlled. As an organisation, we place strict control over who can place information on our own website, or who can contribute directly to the press. It is important that these controls equally apply to our use of social media.

3.2. It is important that the DRC is able to use these tools effectively but equally important that our duties to our service users, our legal responsibilities and our reputation are protected.

3.3. Our use of social media applications has implications for our duty to safeguard children, young people and vulnerable adults. There is a duty of care to protect the DRC from any legal action arising from defamation, harassment, libel, or discrimination, and we must operate within the guidelines of the DRC's Equal Opportunities Policy.

4. Scope

4.1. This policy covers the use of social media tools by third parties and contractors acting on behalf of the DRC. These groups are referred hence forth collectively as 'DRC representatives'.

4.2. Where individuals from partner organisations are involved and are acting on behalf of the DRC, they will also be expected to comply with this policy.

4.3. Use of social media applications by employees for personal use only is not addressed by this policy. Staff should refer to the Email-Internet Policy.

4.4. The requirements of this policy apply to all uses of social media tools, which are used for any DRC related purpose and regardless of whether the tools are hosted corporately or not. They must also be considered where DRC representatives are contributing in an official capacity to social media tools provided by external organisations.

4.5. Social media tools include, but are not limited to:

- Blogs/Microblogging
- Social networking
- Collaboration networking media
- Social bookmarking
- Photo and video sharing
- RSS aggregation services

5. Terms of Use of Social Media

5.1. Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. The DRC expects that users of social media tools will always exercise the right of freedom of expression with due consideration for the rights of others.

5.2. In particular, Social Media must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the DRC into disrepute.

5.3. DRC representatives should identify themselves as such where appropriate on social media tools. This would include providing additional and appropriate information in user profiles.

5.4. DRC representatives should ensure that any contributions they make are professional and uphold the reputation of the DRC and are in accordance with the conditions of this policy.

5.5. DRC representatives must abide by the conditions of use imposed by any provider of social media they wish to use, eg Facebook, Twitter etc.
5.6. Where a social media provider imposes restrictions on corporate participation that are more stringent than those regarding individuals, council representatives must never attempt to circumvent this by assuming an individual identity.

6. Data Protection

6.1. The DRC's obligations under Data Protection legislation are significant, and are aimed at protecting individuals from any damage through inappropriate capturing, maintaining or disclosure of information. Penalties for breaching data protection legislation are significant.
6.2. The capacity to reach a worldwide audience with instant communication through social media means that there is a significant data protection risk associated with its inappropriate use.
6.3. In managing a social media tool DRC representatives may publish or refer to material from a wide range of sources. Equally, DRC representatives may receive comments, enquiries or complaints from members of the public through social media.
6.4. Both published and received material may contain personal data. The DRC is committed to full compliance with the law and to the welfare of individuals and therefore any such personal data should be treated with care.
6.5. Anyone processing personal data must comply with the principles of good practice contained that relate to material published and correspondence received.
6.6. Material published through social media is potentially accessible to anyone in the world. It is essential to restrict the publication of personal data, which includes facts and opinions about individuals. Only that data for which explicit consent for publication has been obtained, or that is clearly already, and properly, in the public domain can reasonably be published.
6.7. Correspondence using social media creates electronic records and, as such, individuals are entitled to access these records if they hold information about themselves.
6.8. In the event of a "Subject Access Request" being made by an individual, DRC Representatives will be required to provide copies of relevant emails. All requests must be satisfied within 40 calendar days of receipt of the request.
6.9. DRC Representatives must consult the Chief Officer wherever they feel that social media activity may have implications with regard to Data Protection legislation.

7. Safeguarding Vulnerable People

7.1. Representatives of the DRC must bear in mind that the information they share through social media, including through private spaces, remains subject to legal requirements governing publication and disclosure, including the Safeguarding of Vulnerable Groups Act (2006).
7.2. Any use of a social media tool that is specifically targeted at engaging with young people, or other vulnerable people including vulnerable adults needs to be mindful of good practice guidance, including advice from St Helens Safeguarding Children Board, and St Helens Safeguarding Adults Board.

7.3. On-line communication brings risks that include contact with people who may wish to cause offence or harm, cyber-bullying through images and messages, and access to obscene or offensive contact.

7.4. The use of social media to engage with young people should not target potential users who are under the minimum age of the service being used, nor should users be asked to divulge any personal details including home and e-mail addresses, telephone numbers or anything that may identify the location of the person.

7.5. E-safety issues can potentially affect all people who use online services, particularly those who may be at a higher risk of being persuaded to share sensitive personal information

7.6. e-Safety awareness is available for professional staff who may be at risk of misrepresentation and malicious accusations through social networking.

8. Obligations under Equalities Legislation and the reporting of hate crimes

8.1. Social Media must not be used in an abusive or hateful manner, or in such a way that breaches the DRC's obligations under equality and diversity legislation (Race Relations (Amendment) Act 2000)

8.2. This includes the content of public and private social media tools. It includes messages, images or other information that may be posted by DRC representatives. Importantly, it also covers the hosting of posts by other parties on social media sites relating to DRC activity.

8.3. Where the DRC receives electronic material through social media that is in contravention with legislation in respect of Hate Crime, or incitement to such, we will report this to the Police without hesitation or exception.

9. Responsibilities regarding potential criminal activities

9.1. The DRC is bound by the legislative requirements of the Anti-Terrorism, Crime And Security Act 2001 to report to the police any activity, or suspicion of activity relating to terrorism or incitement to such that may arise through our use of social networking tools.

9.2. The DRC may also share with the police any information regarding actual or potential criminal activity of any kind received through social media.

10. Obscene Publications

10.1. The publication of obscene material is prohibited by the Obscene Publications Act 1959; the Protection of Children Act 1978 and the Criminal Justice Act 1988)

10.2. This legislation will apply to material and images that may be posted by third parties on social networking sites hosted by the DRC.

10.3. Arrangements must be in place to prevent the DRC from hosting any such material or images posted by third parties on hosted social networking sites.

11. Code of Conduct for Employees

11.1. Social media must not be used in a manner that breaches the DRC's misconduct and bullying and harassment policies.

11.2. Employee use of personal social networking tools should be for DRC business purposes only, and is governed by the Email-Internet Policy.

11.3. In particular, DRC representatives should never use a DRC e-mail address for personal use of social media networking.

12. Use of User-ID's and e-Mail Addresses and Council Branding

12.1. DRC representatives must only use @deafnessresourcecentre.org email for user accounts that will be used for official DRC purposes, unless this is specifically prohibited by the application being employed;
12.2. In certain circumstances (e.g. www.facebook.com), alternative email accounts can be used username logins only and must never be displayed on any website or otherwise made public.
12.3. The use of the DRC's logo and other branding elements should be used where appropriate to indicate the DRC's support.
12.4. The logo, or other devices must never be used on social media tools that are unrelated to, or are not representative of, the DRC's official position or which do not conform to the conditions within this Policy.

13. Feedback, Complaints and Requests for Information

13.1. Appropriate feedback and complaints information must be published in a prominent place, which is easily accessible to other users.

13.2. Service requests, complaints and comments made by users via social media tools should be referred to the correct DRC department. Communication regarding these enquiries must not be dealt with through social media. Only direct communication methods, such as e-mail and telephone can be used, in accordance with professional standards.

13.3. The Freedom of Information Act 2000 may apply to requests received through Social Media. This may require DRC Representatives to disclose information when presented with such a request. Any request made by users via social media should be referred to the Chief Officer. Communication regarding these enquiries must not be dealt with through social media. Only direct communication methods, such as e-mail and telephone can be used, in accordance with out professional standards.

13.4. Requests for statements from the DRC or press enquiries through social media should be referred directly to the Chief Officer, and managed accordingly.

14. Publication of Music, Images and Video Clips through social network sites

14.1. Any music, image or video footage published by DRC representatives through a social media outlet must be from an appropriate and approved source.
14.2. DRC representatives must ensure that images or audio and visual material published through a social media outlet do not infringe copyright requirements.
14.3. DRC representatives must be mindful of the need for permission and consent where images of individuals, particularly children, are shared through social media.

15. Copyright

15.1. DRC representatives are required to comply with copyright law when copying / using any image or other digital representation. DRC representatives must assume

that any material or works they seek to distribute or display via social media is protected by copyright unless they can specifically demonstrate otherwise

15.2. As such, only images, music, video presentations and other material from trusted sources may be displayed or distributed via social media.

16. Moderation of Social Media Tools

16.1. A Social Media Moderator is one of the most important and difficult roles to undertake. The main role for the allocated moderator will be to see that any comments posted comply with the guidance provided to participants and allow the DRC to conduct social media activity in accordance with this policy.

16.2. The Moderator will be the individual who ensures that no material is published, either by ourselves *or by third parties*, that will contravene our responsibilities under this policy, in particular:

- disclosure of personal information in contravention of the Data Protection Act;
- material of an offensive nature;
- images of a pornographic or otherwise offensive nature;
- material that is of a racial, homophobic or otherwise discriminatory nature, and that may constitute incitement;
- material of a defamatory nature;
- material that breaches our safeguarding responsibilities; and
- any other inappropriate material of the type considered in section 4 above.

16.3. Moderation needs to be appropriately resourced, in particular on 'open forums' where third parties may post material directly for public viewing at any time of the day or night.

16.4. Where access to a site is open to a wide community, without the need to register, and where users may post material directly for public view (eg Facebook, Twitter), the risk of carrying inappropriate or offensive material is greatest, and moderators need to be vigilant in frequently checking posted material and removing offending posts as soon as possible. This is particularly important when using Twitter, as although 'tweets' can be deleted, this may occur after they have been forwarded ('re-tweeted') to many other users from our feed.

17. Security and Access Controls

17.1. The capacity to broadcast damaging material and images across the world in an instant means that access to our social media output needs to be controlled in the same way as access to our website.

17.2. All moderators, administrators and users of social networks need to ensure that they log out of all social media tools immediately after use.

17.3. All moderators, administrators and users of social media need to ensure that their username or password are never saved or stored on their PC's, laptops, mobile phones or other devices.

17.4. All moderators, administrators or other users with access to social media on behalf of the DRC need to ensure that they only post material to public view from an

appropriate, professional and private environment. This is particularly important when material is being created or moderated from outside the office environment.

17.5. Anyone posting material on behalf of the DRC needs to consider that they will be accountable for the quality and content of this material under the terms of this Policy when determining where and when they post that material.

18. Social media approval process

18.1. All proposals for services to use social media tools (whether they are hosted by the DRC or by a third party) must be approved by the Chief Officer or in their absence; the Senior Manager for the service

18.2. Where use of social media is proposed for the purposes of marketing and communication, proposals must form part of a relevant marketing and communications plan or campaign for the service, consistent with the DRC 'brand'.

18.3. Where use of social media is proposed for the purposes of consultation, this has to be approved and be consistent with the DRC 'brand'.

18.4. Each application must be detailed and specific. Supporting information must include:-

- The Social Media tool that applicants are seeking to employ;
- Who will be responsible for administering all aspects of the social media proposal, including the monitoring of user activity and/or comments.
- How Moderation will work

19. Enforcement

19.1. The Chief Officer / Senior Manager reserves the right to require the closure of any applications or the removal of any content published by DRC representatives which they deem may adversely affect the reputation of the DRC or place it at risk of legal action.

19.2. Any breach of this Policy could result in the use of the social media tool or offending content being taken away, and the publishing rights of the responsible DRC representative being suspended or permanently removed.

19.3. Any communications or content that causes damage to the DRC, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the DRC's Disciplinary procedures apply.