DELIVERING MENTAL WELL-BEING SERVICES ONLINE

ramp

Risk Awareness and Management Programme

Foreword

As a unique group of organisations working together to bring psychological therapies to the NHS and improve access for all who need them, the New Savoy Partnership is delighted to support the Risk Awareness and Management Programme (RAMP). Our joint mission is to ensure people of all ages and backgrounds who need psychological therapy can have appropriate and timely support, delivered by therapists with the right skills, through the NHS.

As a group of organisations committed to excellence in the quality of the services we offer it is appropriate to have a document such as this, which provides guidelines on good practices to organisations delivering mental well-being services online.

People know they have to take responsibility for their own mental health, and the digital world offers an unprecedented opportunity for those bearing the distress of an emergent or existing mental health problem to find support and information at the earliest possible stage. However, people often also need, expect and are entitled to support from mental health services during their journey towards recovery. To date, there can only be a limited confidence in what they discover online. For many people it will often be difficult to distinguish the helpful from the less so. And for commissioners and clinicians it will often not be easy to navigate their way in a fast-moving market.

The RAMP initiative is relevant to mental well-being providers who wish to offer the highest quality of online services, and to people who wish to find and choose support that suits them, knowing it will meet approved standards.

I warmly thank those who have worked hard to produce these guidelines, and commend them to you as an important contribution towards realising the ambitions of the New Savoy Declaration.

Jeremy Clarke, Chair of the New Savoy Partnership

Table of Contents

Foreword 1
Authors and Contributors 3
Supporters and Sponsors 4
About RAMP 5
Introduction 6
Benefits of mental well-being services being more accessible online 7
Risk Awareness and Management Program 8
Online therapeutic service provision may involve one or more of the following: 9
Four Key Areas of Responsibilities for Providers 10
RAMP and the four categories of risks associated with online interactions 11

1. Data Protection and Respect of Personal Information 14
   General guidance and resources 15
   Risks of failing to address risk in relation to data protection and privacy include: 15
   Table 1.0: Data Protection Risk Awareness and Management Programme to manage key risks in relation to Content 16
   Table 1.1: Data Protection Risk Awareness and Management Programme to manage key risks in relation to Contact 17
   Table 1.2: Data Protection Risk Awareness and Management Programme to manage key risks in relation to Conduct and Commerce 18

2. Informed Consent 19
   General guidance and resources 20
   Consent to have data processed 20
   Consent in relation to treatment 20
   Risk of not having effective consent procedures in place 21
   Table 2.0: Informed Consent: Risk Awareness and Management Programme to manage key risks in relation to Content 22
   Table 2.1: Informed Consent: Risk Awareness and Management Programme to manage key risks in relation to Contact 23
   Table 2.2: Informed Consent: Risk Awareness and Management Programme to manage key risks in relation to Conduct and Commerce 24

3. Privacy and Safety: Equipping users with knowledge and tools 25
   General guidance and resources 26
   Privacy preserving settings 26
   Privacy preserving user actions 26
   Sharing content safely 26
   Privacy and safety both online and offline: Geo-location data 28
   How to use location services more safely 28
   Limit who knows your location 29
   Risks of failing to address risk in relation to safeguarding user safety 29
   Table 3.0: Privacy and Safety: Risk Awareness and Management Programme to manage key risks in relation to Content 30
   Table 3.1: Privacy and Safety: Risk Awareness and Management Programme to manage key risks in relation to Contact, Conduct and Commerce 31

4. Moderation 32
   General guidance and resources 33
   Table 4.0: Moderation and reporting pathways: Risk Awareness and Management Programme to manage key risks in relation to Content and Contact 35
   Table 4.1: Moderation and reporting pathways: Risk Awareness and Management Programme to manage key risks in relation to Conduct and Commerce 36
   Appendix: 37

Authors and Contributors

Principal author

Dr Rachel O'Connell, independent consultant

Co-authors

Jane Chapman, Governance and Risk Adviser, Tavistock and Portman NHS Foundation Trust,
Dr Richard Graham, Consultant Psychiatrist, Tavistock and Portman NHS Foundation Trust

Editor

Sharon Novara -Tavistock and Portman NHS Foundation Trust

Contributors

Dr Kate Anthony, FBACP. CEO, The Online Therapy Institute

John Carr - Children's Charities' Coalition on Internet Safety

Derek Chambers - Director of Policy and Programmes of Inspire/ReachOut.ie

Helen Coles - Head of Professional Standards, British Association for Counselling Psychotherapy

Carole Hirst - Clinical Director of Psychological Therapies, Rotherham, Doncaster &
South Humber NHS Foundation Trust

Jenny Hyatt - CEO Big White Wall

Lizzie Cartwright - Web and Social Media Specialist - Individual Giving at NSPCC

Ruth Ní Eidhin - Communications Officer, Bodywhys - The Eating Disorders Association of Ireland

Anna Lally - Deputy CEO SpunOut.ie

Andy Osborne Drugs.ie

Supporters and Sponsors

Supporters

New Savoy Partnership http://www.newsavoypartnership.org/

UK Council for Child Internet Safety

Young and Well: Cooperative Research Centre for Young People, Technology and Wellbeing

Sponsors

Facebook

Tavistock and Portman NHS Foundation Trust

British Association for Counselling Psychotherapy

Vodafone

About Ramp

The Risk Awareness and Management Programme for Delivering Mental Well-being Services Online has been developed on a voluntary, collaborative self-regulatory basis by the organisations listed on the Contributors page. The Programme offers good practice recommendations for the providers of online mental well-being services to enhance the safety of people using their services.

The Programme outlines the risks that mental well-being providers should be aware of and offers guidance with respect to how to mitigate those risks. The guidance is not intended as a 'one size fits all' solution. It is recognized that online mental well-being service provision is an emerging field, populated by both statutory and non-statutory providers. Online mental well-being providers can vary greatly in terms of the type of service they offer users, the platforms on which they can be consumed, their ideological underpinnings and their user demographics. All of these factors affect the levels and types of risks that are attendant to those services and the strategies that may be appropriate and reasonable to address such risks.

Accordingly, in determining their own safety strategies, online mental well-being providers that support RAMP take into account the particular nature of their services in order to apply the relevant recommendations. Therefore, while Contributors have reached consensus on this first iteration of RAMP, it is for each provider to judge where and how far to apply the document's specific recommendations.

The RAMP guidelines are aspirational and not prescriptive or legally binding but are offered to mental well-being providers with a strong recommendation for their use. The guidelines are the culmination of work conducted by a range of mental well-being providers over a number of years. This latest iteration of the guidelines is regarded as a work in progress and will be subject to review and updating at regular intervals. We recognise that it cannot be comprehensive, given the rapid developments within the digital world, and RAMP is best considered as a developmental tool or programme that assists those learning about the digital world.

The Programme complements existing good practice guidelines, - see appendix A - which collectively aim to shape a consistent and complementary framework on which providers can build and develop strategies to support and protect service users.

Introduction

- The Risk Awareness Management Programme (RAMP) is intended to serve as a guide for organisations that have, or are considering, extending or enhancing online mental health and social support service provision in a safe and secure manner.
- The Programme is also aimed at social networking service providers, mobile operators, gaming platforms and application developers interested in encouraging mental well-being organisations to signpost and/or deliver support services from within specific online environments.
- In addition, the Programme will be of interest to regulators, policy makers and academics, who have an interest or remit in the broader e-health area.
- The Programme is intended to form the basis of discussions about the development of online mental well-being services between commissioners and mental well-being providers from which a contract for services can then be agreed.
- We recommend that accredited service providers, registered charities, government endorsed service providers, commissioning and funding organisations use the guidelines as appropriate for the planned level of service provision in the development of interactive online support services.

The presence of, for example, pro-anorexia, pro-suicide and pro-self-harm sites, where people interact in such a way that self-destructive behaviours can be reinforced, highlights the need for high quality, alternative sources of information and support online. Interactions with online mental well-being providers can increase one's digital resilience and reduce the likelihood of engaging in harmful behaviours. Furthermore, activities such as cyber-bullying or the online solicitation of minors involve leveraging a victim's vulnerabilities for the purposes of harm or exploitation. These vulnerabilities to date include: poor mental health, concerns about body image, high levels of risk-taking and low self-esteem. The accessibility of social support and mental well-being services online, 24/7, provides users with opportunities to seek advice and support from appropriate sources, thus increasing resiliency and decreasing the likelihood of victimisation.

Individual seeking of help online may lead to an increase in the encouragement of friends facing similar issues to access online mental well-being services. These potential outcomes underline the value of mental well-being providers having a high quality online presence. This will also help to ensure that organisations remain relevant to, and continue to reach their target audience.

Increasingly, social media and gaming platforms, application developers and mobile operators are forming partnerships with online mental well-being service providers to facilitate therapeutic service delivery.

There is a broad spectrum of well-being service provision from e.g., daily positive messages through to therapeutic counselling. From a safeguarding perspective, it is not advisable to deliver a therapeutic service on a general audience, social networking platforms based on real identities. However, it may be worthwhile exploring the embedded features on various online platforms, e.g., Skype and to contact relevant partner companies to discuss possible collaborations. It is important to be aware that third-party services that offer direct communication channels often provide limited security and privacy, which could result in exposure of confidential client data to third parties. Providers should consider use of encryption security or the equivalent for therapeutic communication. All communications between a mental well-being provider and users may become a part of the clinical and legal record. Providers should define the record according to the laws of their jurisdiction and according to their defined professional scope of practice.

It is important to conduct a Risk Awareness and Management Programme analysis on each communication channel and to inform users accordingly.

The prevailing wisdom is that users seeking mental health support online have greater access and are better protected when they can use an avatar or a pseudonym and remain anonymous, or when the audit trail of contact with mental well-being providers is not easily accessible to other people.

BENEFITS OF MENTAL WELL-BEING SERVICES BEING MORE ACCESSIBLE ONLINE

BENEFITS OF MENTAL WELL-BEING SERVICES BEING MORE ACCESSIBLE ONLINE

The benefits of the increasing number of mental well-being services having a presence online are manifold and include:

- Increased accessibility of support services, particularly for people living in remote areas where counselling services are not easily accessible, or appointments with counsellors can only be accommodated weeks or months after the initial request for help.
- Online services are beneficial for people who are unable to leave home and for those who would ordinarily not seek face-to-face counselling or therapy.
- Placing services in online locations, where people are spending increasing amounts of time can help to normalise the use of support services and de-stigmatise early help-seeking.
- Online counsellors and the use of online mental well-being services reduces the visibility of seeking help, this can also be helpful in reducing social stigma, particularly within communities who have a negative perception of services.
- Greater choice of support options may offer users a wider selection of therapists to choose from; this is beneficial for persons looking for a counsellor or therapist with specific experience, or with a particular language, religious or cultural understanding. Users can also connect in an online therapeutic environment with other people who are dealing with similar issues.
- More generally, the accessibility of advice and support services, designed to mitigate the risks that people may encounter online, increases Internet users' personal safety and sense of well-being.
- Increasing the delivery of mental well-being services online can ensure that Department of Health strategic goals are met.

Mental well-being organisations should conduct a thorough strategic needs-analysis to determine the following:

- the online channels most appropriate for the target audience
- staff training needs
- financial and capacity building requirements
- what systems are in place to monitor and evaluate the effect of changes to service delivery?

It is important to define the purpose of any online presence e.g. counselling, awareness raising, signposting, fund raising or a partnership with an online platform. This will help to inform the decision making with respect to the application of the guidelines, which is outlined in the Risk Awareness and Management Programme for each context.

Risk Awareness and Management Programme

Safeguarding users of Internet well-being services (particularly users who are children, young people or vulnerable adults) must be a top priority to developers of systems and programmes and those who are purchasing or accessing them.

In the following sections the Risk Awareness and Management Programme is described in practical detail to assist developers and providers self assess their online therapeutic services and determine what additional actions they may need to make in order to be confident of providing a service where risks to users have been eliminated or mitigated as far as possible.

Online therapeutic service provision may involve one or more of the following:

- **Psycho-education sites** and applications provide a user with knowledge about a particular psychological issue or condition, the likely causes of that condition, and the reasons why a particular treatment might be effective for reducing their psychological distress. Information is usually 'searchable'. In addition, a mental well-being organisation may or may not choose to afford interactivity, such as the ability to post comments or discuss issues.
- **Supervised peer-to-peer mentoring:** Peer mentoring has been shown to increase resistance to stress-related anxiety and depression and it is regarded as one of the most successful approaches to encouraging people to seek help, for example, to manage eating disorders.
- **Online Computerised Cognitive Behavioural Therapy (CCBT)** delivers cognitive behavioural techniques to a computer-user to increase successful coping strategies and improve mental well-being. The National Institute for Clinical Excellence (2006) describes CCBT as a "generic term for delivering CBT via an interactive computer interface delivered by a personal computer, Internet or interactive voice response system".
- **Asynchronous or Synchronous Counselling/Psychotherapy Services:** Psychotherapy, or personal counselling with a psychotherapist, is an intentional interpersonal relationship used by trained psychotherapists to aid a client or patient in problems of living. It aims to increase the individual's sense of his or her own well-being. Psychotherapy may be performed by practitioners with a number of different qualifications, including psychiatry, clinical psychology, counselling psychology, mental health counselling, music therapy, art therapy, drama therapy, dance/movement therapy, rehabilitation counselling, occupational therapy, psychiatric nursing, psychoanalysis and other psychotherapies. It may be legally regulated, voluntarily regulated or unregulated, depending on the jurisdiction. Requirements of the profession vary, but often require graduate school and supervised clinical experience. In the UK, the main professional organisational body will require post-graduate training in the provision of online mental health for members wishing to identify themselves as an online service provider.

Online therapeutic service provision in each of the four categories described above will involve differing levels of legal oversight, safeguarding principles, duty of care requirements and good practices.

Mental well-being providers regularly opt to commission the development of, or operate a bespoke, online therapeutic service delivery platform. This allows mental well-being providers the opportunity to meet the needs of service users while ensuring the organisation can safely meet the legal, ethical and safeguarding requirements in a manner that the organisation deems most appropriate. The type of online platform and functionality chosen will vary with respect to the nature, scope and extent of legal, ethical and good practice requirements involved in the extending of service provision online and the nature of the interactions that can be expected to occur.

Mental well-being providers may also wish to consider having a presence on one or more online platforms that are owned and operated by Internet, mobile and/or gaming companies that are utilised by a general audience. The purpose of these 'satellite' online presences can include the following valuable if non-therapeutic activities:

- Awareness raising
- Fund raising
- Advertising and signposting
- Campaigning

There are a number of possible different configurations of service delivery, communication channels and online presences and it is therefore appropriate for each organisation to conduct a RAMP analysis and decide on what would work best. For example, a mental well-being provider may decide to have a 'satellite' online presence for the non-therapeutic purposes outlined above before providing an online therapeutic service. However, in every instance of online provision it is important to work through the RAMP analysis so that appropriate policies and procedures are in place. It is especially important to recognise that users may disclose personal and sensitive information on a non-therapeutic platform and mechanisms need to be in place to manage those instances, especially concerning risk to self and others. In addition, it is also important to devise maintenance and/or exit strategies when, for example, a campaign ends and a satellite presence can no longer be monitored. Users should be provided with clear information and signposted to the appropriate place to find support.

Unfortunately, the breadth of options for service provision means that there is not a 'one size fits all' approach that can be adopted by mental well-being providers. Therefore each service provider should conduct a thorough Risk Awareness and Management Programme analysis to ensure that the key issues have been considered carefully in relation to any extension of one or more aspects of a mental well-being service online.

Four Key Areas of Responsibilities for Providers

RAMP has been set out to cover the four key responsibilities of providers and whilst in practice each of these areas of responsibility is interlinked with the others, this approach will help providers consider in a systematic way whether they have sufficient and effective ways of managing the key risks for users.

The four subsections of the Risk Awareness and Management Programme are as follows:

Data protection and Respect of Personal Information: Mental well-being professionals have a number of legal obligations to protect the personal information of individuals under the *Data Protection Act 1998*. Laws governing data retention periods vary between regulated mental health providers and other well-being providers and it is important that users are adequately informed of this. Mental health professionals also have an ethical responsibility to safeguard users from unauthorised disclosures of information.

Privacy and safety: Mental well-being professionals should be committed to ensuring the safety of users. Services should be operated in a manner that preserves and values an individual's privacy. Usually, users should be provided with a range of privacy setting options, with easy to understand supporting information that encourages users to make informed decisions about the level of information they post online.

Informed consent: Clients should be adequately informed about the nature of the services being offered. Practitioners should obtain appropriately informed consent from their clients concerning any intervention, and respect a client's right to decide what they wish to do. The process of ensuring informed consent involves clearly outlining the nature of the service being offered and respecting a client's right to choose whether to continue or withdraw. It is also important to be clear about the situations in which confidentiality could be breached. Providers should work towards ensuring that services are sensitive to the developmental or other needs of the intended audience.

Moderation and reporting pathways: Mental well-being providers should adhere to professional good practice or ethical guidelines with respect to user-counsellor and group interactions. Providers should ensure that users are adequately informed about what to expect from a service. Moderation can encompass peer-to-peer mentoring and user interactions. A document entitled 'Good practice guidance for the moderation of interactive services for children'[14] is a valuable resource for mental well-being providers. Establishing clear reporting pathways is essential to ensuring the safe operation of online mental well-being services.

Questions RAMP is designed to address:

1. What risks to a user and a provider are associated with online mental well-being service provision?
2. What safeguards need to be put in place so that users and providers can be confident about the service?
3. What safety measures, systems and processes are required to make this happen?

It is important to bear in mind that the answers to these questions may differ depending on the online channel being used.

[14] 'Good practice guidance for the moderation of interactive services for children' - https://docs.google.com/viewer?url=http%3A%2F%2Fmedia.education.gov.uk%2Fassets%2Ffiles%2Fpdf%2Fi%2Findustry%2520guidance%2520%2520%2520moderation.pdf

RAMP and the four categories of risks associated with online interactions

RAMP explores the four areas outlined above in the context of risks commonly associated with online interactions, i.e. the "4C's", as follows:

Content risks involve inaccurate, harmful and illegal content. The Internet is home to a wealth of information, but not all of it is factually accurate. When people share information about mental health it is not always possible to ensure the accuracy of the content users see online. Not all content shared will be suitable for users of the service. It may cause offence, be degrading to others, and cross the boundaries of what most people would deem to be acceptable. An online mental well-being service may afford access to a wealth of information and resources, and so users need to take a personal responsibility to ensure that the content they post is appropriate and legal for others to view. Users may also choose to disclose personal, sensitive information about themselves or other users of the service that could make them vulnerable to a range of risks, and operators of mental well-being services need to be alert to these risks. The Internet also provides a means of sharing links to download data. Music, movies and games can all be downloaded. However, not all downloads are legal. Downloading software, games or music from illegal sites is a criminal offence.

- To mitigate against these types of risks it is important that providers of online well-being services ensure they establish clear house rules for users that address the issue of what constitutes inappropriate content in the context of a specific online well-being service.
- Remember that an employer is liable for the conduct of employees if the conduct occurred within the scope of his or her employment. If you operate an online well-being service in which employees are allowed, and even encouraged to post information, the employer could be liable if the employee posts something inappropriate. Therefore it is important to develop and enforce a social media policy for employees. This policy can be posted online and will be very specific to the culture of the organisation. It is important to clearly state in your organisation's Terms of Service the penalties associated with misuse of the service.
- Be careful of endorsements of products and services. Employees can be allowed to endorse the company they work for, their co-workers and products and services provided. However, if the employee's identity is not disclosed in an endorsement, it is deceptive, and may violate standards defined by the Office of Fair Trading.
- With respect to illegal and allegedly illegal content posted online e.g. images of child abuse and unlawful hate speech, it is important to establish clear policies and procedures to handle illegal content. The Internet Watch Foundation is the only recognised non-statutory organisation in the UK operating an Internet 'hotline' for the public and IT professionals to report their exposure to potentially illegal content online: http://www.iwf.org.uk/

Contact risks involve inappropriate and unwanted contact between users. This includes any contact in which one user may exploit another, such as an adult with a sexual interest in children and contact by young people who solicit other young people on behalf of those adults.

1. To mitigate against this type of risk it is important that providers of online well-being services ensure that staff who have access to information about, or interact with, service users are vetted and that appropriate safeguarding mechanisms are put in place to mitigate the risk of an abuse of trust, and/or inappropriate contact.
2. It is important to be vigilant with regard to inappropriate contact between service users. Users of online well-being services should be able to access straightforward mechanisms to report matters that concern them.
3. In addition, mental well-being providers should establish clear reporting mechanisms with law enforcement agencies. Mental well-being organisations should cooperate with national agencies, such as the Child Exploitation and Online Protection Centre, www.ceop.gov.uk, to report suspected online solicitation. With respect to suspected risk to life of an online user well-being providers should have a memorandum of understanding with the police telecommunications unit.

Conduct risks relate to how people behave online. With the interactivity that web 2.0 technologies enable, it is important to remember that in addition to being victims people can also initiate or participate in anti-social or criminal activities. Behaviours can include bullying or victimisation (behaviours such as spreading rumours, excluding peers from one's social group and withdrawing friendship or acceptance) and potentially risky behaviours (which may include for example divulging personal information, posting sexually provocative photographs, impersonation, lying about age or arranging to meet face-to-face with people only previously met online). To mitigate against this type of risk it is important to set clear guidelines for staff and service users in relation to how to model good conduct themselves when interacting online and to provide robust reporting mechanisms for users and clear reporting escalation pathways to law enforcement agencies if there is a suspected risk to life or illegal conduct.

Commercial risks refer to the risk of users being tricked or encouraged into giving out financial information that could be used to defraud. This risk may be of particular importance to mental well-being services based on a fee paying model or where the service is funded through revenue from advertising, or where users' data is sold on to e.g. advertisers or pharmaceutical companies in the absence of users' consent or in a non-aggregated and identifiable state. It can also refer to an organisations' databases becoming compromised and a user's financial and personal information being accessed illegally. This would compromise a user's personal safety and well-being and could even lead to financial loss. It can also refer to, in the case of young people, harm associated with being exposed to inappropriate advertisements. To mitigate against these types of risks providers need to ensure they apply security measures to protect users' personal data and protect against SPAM. Privacy policies should clearly state how users' data will be used to ensure that advertising and marketing is in line with the relevant advertising codes.

The RAMP specifically identifies the potential risks associated with online interactions from both an online mental well-being provider's and user's perspectives and outlines the measures that need to be implemented to mitigate those risks. It is designed to support online well-being providers seeking to build risk management programmes and techniques into their products and then to self-regulate these in order to provide assurance on users safety.

Definition used in this section

Risk: Risk is defined as 'the chance of something happening that will have an effect on an objective'. It is measured in terms of impact and probability.

Mitigating risk: (i.e. reducing the chance of a risk having an effect) actions taken to reduce either the impact or the probability (or both) of the risk having an effect on an objective.

"4 T's": At the simplest level there are four actions that can be taken when considering a risk; these are shown in the box on the right hand page

Actions which can be taken to mitigate risk	
Terminate	Stop the activity that is causing the risk, such so that it cannot occur
Tolerate	Accept the risk, when the risk is considered to be at an acceptable level and nothing further can be done at a reasonable cost to reduce the risk to a lower level
Treat	Take action to mitigate the risk either by reducing the probability of the risk occurring and/or the impact of the risk if it does occur. (Treating risks can be achieved by a whole range of actions, for example: training, effective policies and procedures, audits, clear user information, instruction, etc.)
Transfer	Pass the risk to someone else e.g. by insurance or passing responsibility for the risk to a contractor, or making it clear to a user that they are accepting the risk

Acceptable level of risk: Each provider will need to determine what is an acceptable level of risk for their organisation setting. This is most easily achieved by adopting a risk matrix approach, where different risk combinations can be graded to determine the level of action that needs to be taken. The provider will need to set definitions for high medium and low impact and probability on terms that are relevant to their service.

A simple risk matrix is shown below:

PROBABILITY	High	3	6	9
	Medium	2	4	6
	Low	1	2	3
RISK MATRIX		Low harm	Medium harm	Severe harm
	IMPACT			

Actions to be taken in response to risk rating	
High Risk	Action must be taken to mitigate risk
Medium Risk	Risk mitigation must be reviewed to confirm all reasonable steps to mitigate risk are being taken and then risk can be tolerated
Low risk	Risk can be managed by routine procedures , unlikely to need further resources to reduce risk, risk can be tolerated

1. DATA PROTECTION AND PRIVACY POLICY

DATA PROTECTION AND RESPECT OF PERSONAL INFORMATION

General guidance and resources

If your organisation handles personal information about individuals there are a number of legal obligations to protect that information under the Data Protection Act 1998. There is a statutory requirement for every organisation that processes personal information to notify the Information Commissioner's Office (ICO), unless they are exempt. Failure to notify is a criminal offence.

To access a helpful guide regarding notification and to assess whether or not your organisation might be exempt see section 6 of the guide produced by the ICO, see link:

http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/notification_handbook_final.ashx

Sector guides have been created by ICO and charities can access information at http://www.ico.gov.uk/upload/documents/think_privacy_charities/ico_think_privacy_toolkit_charities.pdf

The health sector can access a sector guide at

http://www.ico.gov.uk/for_organisations/sector_guides/health.aspx

The ICO has also produced helpful guides with respect to data sharing – see http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx

The Charity Commission[15] states that charity trustees are responsible for ensuring that those benefiting from or working with their charity are not harmed in any way through contact with it. They have a legal duty to act prudently and this means that they must take all reasonable steps within their power to ensure this does not happen. It is particularly important where beneficiaries are vulnerable persons or children in the community. Trustees are expected to find out what the relevant law is, how it applies to their organisation and to comply with it where appropriate. They should also adopt best practice as far as possible. Children are an especially vulnerable group and therefore the Charity Commission is concerned to stress the importance of charities having proper safeguards in place for their protection.

Client confidentiality is a major concern in the provision of counselling services. Clients who communicate deeply felt and/or possibly shameful (to them) thoughts and feelings online, via email, chat, IM, forum, VoIP, Video, Virtual World Environments, will have concerns about the deliberate or accidental disclosure of these. It is important that computer based electronic records are subject to exacting ethical requirements with regard to storage and disclosure to others. Forthcoming British Association for Counselling and Psychotherapy Guidelines for Online Counselling, Psychotherapy and Supervision, are expected to make encrypted service provision compulsory for online mental health services.

Risks of failing to address risk in relation to data protection and privacy include:

Financial and reputational costs
A data breach can be expensive to put right and will reduce customers' confidence in your organisation. You could receive a monetary penalty of up to £500,000 from the ICO.

A number of complaints, relating to the provision of unencrypted services have resulted in personal identifiable communications being posted on the Internet, which resulted in complaints being brought and against the online therapists.

On 26 May 2011, the Privacy and Electronic Communications (ECDirective) (Amendment) Regulations 2011 came into force. These amend the Privacy and Electronic Communications (EC Directive) Regulations 2003. The 2011 Regulations enhance the Information Commissioners powers and introduce new requirements. The new powers enable the Commissioner to:

- impose civil monetary penalties of up to £500,000 for serious breaches of PECR;
- audit the measures taken by a provider of public electronic communications services (a service provider) to:
- safeguard the security of that service
- comply with the new personal data breach notification and recording requirements
- impose a fixed monetary penalty of £1,000 on a service provider that fails to comply with the new breach notification requirements; and
- require a communications provider to provide him with information needed to investigate the compliance of any person with PECR (a third party information notice).

From a user's perspective the Data Protection Act 1998 has been designed to ensure clients' privacy. Therefore, strong policies on privacy and data protection, backed up by training and clear accountability for staff are essential. Clients need to be able to trust organisations to look after their personal information safely and securely.

[15] http://www.charity-commission.gov.uk/Charity_requirements_guidance/Charity_governance/Managing_risk/protection.aspx

Table 1.0: Data Protection Risk Awareness and Management Programme to manage key risks in relation to Content

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Content	Breach of confidentiality Unauthorised use/ sharing of personal information – including financial information	At point of entry, service users should be informed of the following: • The circumstances under which there are limits to confidentiality • The privacy policy should indicate what information is collected about users and how this information will be stored, used and shared • The Terms of Service / House Rules should indicate what constitutes a breach of acceptable behaviour and the circumstances under which personal information will be shared with law enforcement agencies Users should be provided with information about the following: • How to delete content • How to keep content private • How to report instances of alleged misuse of personal information Users should be informed in a timely manner if a data breach occurs	• Conduct a risk assessment using the Risk Awareness and Management Programme; the findings should be signed off by the senior management team • Register with the Information Commissioner if required • Develop a clear statement of trustee responsibilities in relation to online delivery of services • Devise a strict Data Protection Policy with clear procedures detailed in staff manuals • Ensure that data in locations where users' information may be stored e.g. databases, laptops and USB sticks are encrypted • Adhere to regulations with respect to data retention • Provide users with a privacy policy in an accessible format that contains clear information on data handling and use • Make provisions for financial information to be collected via secure methods in line with industry standards[15] • Conduct regular data protection quality assurance checks and education programmes with staff	

Table 1.1: Data Protection Risk Awareness and Management Programme to manage key risks in relation to Contact

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Contact	Inappropriate advice from unqualified well-being providers	• Users need to be informed and assured about the qualifications and experience of the well-being provider's staff they are likely to encounter online • Users should be informed about the nature and extent of that contact, so that they can make an informed decision whether to engage with the service	• Develop recruitment policies and procedures • Create detailed job descriptions • Ensure appropriate training, monitoring and quality assurance mechanisms are in operation • Provide information for users in an accessible format about the qualifications of staff they will encounter • Provide opt-out procedures for users	
	Lack of processes to address concerns leading to loss of confidence in the service amongst users	• Users need to be provided with a means to report alleged inappropriate contact from professionals and/or other users • Users need to be assured that their concerns will be managed effectively and expeditiously	Ensure that there is systematic monitoring and evaluation of the various aspects of the online service, to maximize the probability that minimum standards of quality are being adhered to • Ensure that there are reporting procedures in place so that users can easily report alleged misconduct by staff and other users • Institute effective complaints handling and investigation procedures, which are subject to quality assurance tests • Liaise with relevant law enforcement agencies	

[15]http://www.businesslink.gov.uk/bdotg/action/layer?topicId=1073920405

Table 1.2: Data Protection Risk Awareness and Management Programme to manage key risks in relation to Conduct and Commerce

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Conduct	Failure to respect user confidentiality and user wishes for personal data	• Users and staff need to feel confident that their data will be handled confidentially and used appropriately and understand how their data will be used	• Clear Data Protection Policy and procedures with respect to the use of and storage of both users' and staff's personal information • Clear record keeping and supervision of practitioners • Information for users on data handling and use in an accessible format	
Commerce	Unauthorised breach of confidentiality	• Users need to be informed explicitly how information that they supply will be used and whether at any time their information may be shared or sold to a third party (e.g. advertisers, researchers, insurance companies)	• Use of data policy and procedures with clear boundaries for use that must be adhered to • Information for users on use of data in an accessible format • Users should be able to opt-out of receipt of marketing messages • Users should be provided with a means to report breaches of confidentiality	

2. INFORMED CONSENT

INFORMED CONSENT

General guidance and resources

The overarching principle is that to be legally valid consent must be sufficiently informed and freely given by a person who is competent to do so. Mental Capacity refers to the ability a person has to make decisions about their life. Some people have difficulties in making such decisions: this is called 'lacking capacity'. Under the Mental Capacity Act (MCA) there are now laws governing who can make decisions on someone else's behalf, which help to safeguard vulnerable people. To find out more, including who to contact if you are concerned, plus an e-learning tool for professionals, please visit the *Mental Capacity Act* page.

In the case of online provision of mental well-being services to children and young people consent refers to two separate but related issues:

1. Legal age to give informed consent to have personal data processed by an online service provider
2. Legal age at which a child is deemed competent to give informed consent with respect to counselling and support options

Consent to have data processed

At what age is a child or young person legally deemed capable of entering into a legal contract with a website? The US Children's Online Privacy Protection Act legislation pinpoints the age at 13+. In Europe the Data Protection Act 1998 does not itself explicitly deal with the issue of obtaining consent from children. However, the UK Information Commissioner has written:

"Websites that collect information from children must have stronger safeguards in place to make sure any processing is fair. You should recognise that children generally have a lower level of understanding than adults, and so notices explaining the way you will use their information should be appropriate to their level, and should not exploit any lack of understanding. The language of the explanation should be clear and appropriate to the age group the website is aimed at. If you ask a child to provide personal information you need consent from a parent or guardian, unless it is reasonable to believe the child clearly understands what is involved and they are capable of making an informed decision"
(The Data Protection Good Practice Note: Collecting personal information using websites).

So, privacy policies should be prominent and simply expressed. A very young child may never be able to give adequate consent, whereas an older child may be able to give adequate consent in many different circumstances. The Information Commissioner goes on to refer to a particular age threshold:

"The Act does not state a precise age at which a child can act in their own right. It depends on the capacity of the child and how complicated the proposition being put to them is. As a general rule, we consider the standard adopted by Trust UK (www.trustuk.org.uk) to be reasonable: 'TrustUK approved web traders recognise children need to be treated differently from adults. They will not market their products in any way that exploits children, nor will they collect information from children under 12 without first obtaining the permission of a parent or guardian. They will not collect personal data about adults from children."

Consent in relation to treatment

Securing consent in relation to a specific mental well-being treatment involves a requirement to ensure that users are informed prior to taking up the service about what is offered, the potential benefits and risks, how any risks are safeguarded against or mitigated and the level to which client confidentiality can be assured.

With respect to children it will be a requirement to secure parental consent in order to treat a child. There is no single law that defines the age of a child across the UK. The UN Convention on the Rights of the Child – ratified by the UK government in 1991 – states that a child "means every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier."[16] In the UK specific age limits are set out in relevant laws or government guidance. There are, however, differences between the UK nations. In addition, some especially vulnerable groups have their entitlement to services extended beyond 18.

Securing parental consent in online environments is not a straightforward process and at this point in time it will most likely involve a real world element e.g. visit to GP, counselling service[17].

[16]Article 1, Convention on the Rights of the Child, 1989

[17]Legal definition of a child NSPCC factsheet http://www.nspcc.org.uk/Inform/research/questions/definition_of_a_child_wda59396.html

It is important to consider who has parental responsibility for a child under the legal age of consent:

The child's birth mother
The child's father if

- Parents are married at time of child's birth or
- The father's name appears on the child's birth certificate or
- The father later marries the mother or has a formal agreement with her

Others may acquire parental responsibility through a court order e.g.

- By adoption
- Local Authority with Care Order

Risk of not having effective consent procedures in place

From an organisational perspective not putting appropriate measures in place to mitigate these risks could result in:

Financial and reputational risk to a provider
If there is harm to an individual who uses the service without being informed of the risks and consequences due to age, or there is a failure to provide adequate information on which a user can make an informed choice.

Avoidable harm to a user
Risk of harm to their personal safety and well-being through use of service that is not fully understood and for which informed consent has not been given.

Table 2.0: Informed Consent: Risk Awareness and Management Programme to manage key risks in relation to Content

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Content	User failing to understand the risks (and benefits) accepts the risks and benefits of accessing the service	• Provision of clear and age appropriate information at the registration stage of accessing service • Provide FAQ's and Help pages for users to access at any time • Present users with safety messages about risks and benefits during use of the service • Capture consent through trusted methods or tick box prior to user being able to proceed with service	• Make details of both the risk and benefits associated with use of the service in a way that users can easily access, understand and make an informed decision on • Develop a consent policy suitable and appropriate for mental well-being provider's specific target audience(s) • Put in place systems to ensure that consent is sought and given prior to providing access to the therapeutic/self-help environment	
	Under age user accessing service with the ability to give informed consent	• Age controls and warnings to guard against allowing underage users to access 'adult' content • Consent process involving parent/guardian (if appropriate)	• Have in place systems to gather age data on users to help identify those underage • Develop an under age consent policy and associated procedures • Information for under age users and their parents/guardian in an accessible and easy to understand format	

Table 2.1: Informed Consent: Risk Awareness and Management Programme to manage key risks in relation to Contact

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Contact	User/staff failing to follow the rules about the extent of consent to use service, resulting in boundaries between users and/or users and staff being breached	• Develop, implement and evaluate a training regime and educate staff about agreed policies and procedures • Regularly monitor how policies and procedures are implemented • Conduct spot checks of user and staff activity • Implement robust and effective follow-up of any incident and/or near miss situations	• Develop, implement and evaluate a comprehensive education and training regimen for staff supplement with a training manual/staff handbook • Ensure that staff adhere to a Code of Conduct that has been designed to reflect the values of the mental well-being organisation • Have a clear set of House Rules for users that set the parameters of acceptable and unacceptable behaviours and ensure that these are enforced by staff • Reserve the right to take action against users/staff who misuse the service	

Table 2.2: Informed Consent: Risk Awareness and Management Programme to manage key risks in relation to Conduct and Commerce

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Conduct	Service provider exceeds boundaries of services consented which puts users at risk of harm	• Clear levels of consent for different aspects of the service • Clear information for users to allow them to make informed choices	• Develop, implement and evaluate a comprehensive education and training regimen for staff supplemented with a training manual/staff handbook • Ensure that staff adhere to a Code of Conduct that has been designed to reflect the values of the mental well-being organisation • Have a clear set of House Rules for users that set the parameters of acceptable and unacceptable behaviours and ensure that these are enforced by staff • Reserve the right to take action against users/staff who misuse the service	
Commerce	Risk to user of the organisations providing personal details and/ or usage details for commercial gain without the express permission of the user	• No evidence of breach of in-house rules on sharing user information	• Policies and procedures that address the use of information • Clear user information about the extent of the consent they agree to when initially signing up to the site	

3. PRIVACY AND SAFETY

PRIVACY AND SAFETY: EQUIPPING USERS WITH KNOWLEDGE AND TOOLS

General guidance and resources

Online mental well-being service providers can offer several ways to help protect users, depending upon the kind of service offered.

Privacy preserving settings

It is good practice to ensure that service providers ensure that users' personal profiles on online mental well-being services are not 'searchable', i.e. do not show up in results from use of a search engine. It is also important that all profiles are private by default, i.e., profile cannot be viewed or the user contacted except by 'friends' on their contact list. Other privacy preserving settings that provide users with greater control over who can access their content include the following:

- Being able to block a user from viewing their profile and 'reject' friend requests
- Giving users the option to allow only direct friends to post comments and content to their profile or to delete unwanted comments
- Giving users the option to pre-moderate comments of other users before being published on their profile
- Providing easy-to-use tools for users to report inappropriate contact from or conduct by another user
- Confidentiality is a vital aspect of a therapist /client relationship. Utilising online interactive services where a number of clients and therapists interact in an online therapeutic setting can present a number of challenges in terms of managing expectations of confidentiality. Users and staff should be provided with clear guidance about the prohibition of the use in the public domain of personal and sensitive information about other people gained in an online well-being context

Privacy preserving user actions

Furthermore, to enhance users' safety, privacy and security, mental well-being providers should consider advising users to maintain separate professional and personal profiles, which also differ from profiles used in online therapeutic settings. To achieve this, mental well-being service providers can advise users to do the following:

- Use different email addresses, screen names, blogs, and websites for each profile
- Do not link real name (or sensitive personal information such as their home and email addresses, phone numbers, or photos) with other profiles that they have created
- Add personal information to their online profiles in therapeutic settings judiciously and avoid cross-references to personal sites
- Some online mental well-being services afford users the opportunity to build separate friends lists - for close friends in real world, new online friends only, i.e. those met in the context of the mental well-being service etc. - so that users can manage what they share within one profile

Mental well-being providers should also advise users about how to utilise settings and options to help them manage who can see their profile, who can make comments, and how to block unwanted access by others.

Sharing content safely

With respect to sharing content with other users of an online mental well-being service it is advisable to suggest the following safety guidelines to users:

- Before you put anything online think about what you are posting, who you are sharing it with, and how this will reflect on your reputation. Would you be comfortable if others saw it? Or saw it ten years from now?
- Talk with your fellow users about what you do and do not want shared. Ask them to remove anything that you do not want disclosed.
- Respect the reputation and privacy of others when you post anything about them on your own pages or on others' pages or public sites. Remove anything that does not honour this.
- Periodically reassess who has access to your pages. Friends change over time; it is okay to review those with whom you are no longer on friendly terms

It is important to reassure users that it is possible restore their online reputation if they feel it has been damaged as a result of their own or other people's actions as follows:

- If you find information about yourself that is inaccurate or misleading, act quickly
- In a respectful way, ask the person who posted it to remove it or correct an error. If it is a correction, ask him or her to include a notice (CORRECTION or UPDATED) right next to the original (incorrect) material
- If the person does not respond or refuses to help, ask the website administrator to remove the digital damage

Advise users to create strong passwords

Creating strong passwords is an important way in which users can protect themselves online. Keys to password strength: length and complexity.

An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 14 characters or more
- The greater the variety of characters in your password, the better
- Use the entire keyboard, not just the letters and characters you use or see most often

Create a strong password you can remember

There are many ways to create a long, complex password and Microsoft has developed the following guide to make creating and remembering passwords easier:

What to do	Suggestion	Example
Start with a sentence or two (about 10 words total) service.	Think of something meaningful to you.	Long and complex passwords are safest.
Turn your sentences into a row of letters.	Use the first letter of each word.	lacpasikms (10 characters)
Add complexity.	Make only the letters in the first half of the alphabet uppercase.	lACpAsIKMs (10 characters)
Add length with numbers.	Put two numbers that are meaningful to you between the two sentences.	lACpAs56IKMs (12 characters)
Add length with punctuation.	Put a punctuation mark at the beginning.	?lACpAs56IKMs (13 characters)
Add length with symbols.	Put a symbol at the end.	?lACpAs56IKMs" (14 characters)

Test your password with a password checker

A password checker evaluates your password's strength automatically.

Try Microsoft's secure password checker.
https://www.microsoft.com/security/pc-security/password-checker.aspx

Privacy and safety both online and offline: Geo-location data

What are geo-location services?

If you have used your phone to find directions or locate a nearby restaurant you have used its global positioning system (GPS) and it is likely that it will be able to pinpoint your location within a close range. Location services can be convenient for automatically adding location information (geotags) to photos.

Some people also use location services to post their locations to social networking sites, such as Facebook.

It is important to advise users to be aware that others can use their location information, too.

Concern for mental well-being service users' personal safety and privacy is not simply confined to the online world. A mental well-being provider that places their businesses as check-in points on geo-location services that allow clients with location based-enabled devices to indicate when they are visiting their offices may compromise client privacy. Mental well-being providers should make clients aware of this potential exposure.

When organising events in the real world, for the purposes of e.g. campaigning, fund raising or awareness raising activities, it is important to consider users' safety. Advice regarding geo-locations services on mobile devices should be provided to users.

The risks of using location services are as follows:

- Services that track your location can be used for criminal purposes—for spying, stalking, or theft
- If messages that share your location are tied to your Facebook account, your network of friends and family will know your location. This may impact on your ability to keep your different online activities separate
- Location information is added to all of the other data about you on social sites and blogs, comments you leave, and so on. It is likely to be permanent and searchable
- The apps and search engine you use may sell your location data to advertisers who might then deliver ads on your mobile phone related to where you are

How to use location services more safely

Advise users to choose from among the strategies below to set the level of privacy that is right for them.

Pay close attention to the settings that use your location:

- Consider turning off features that add location information (also called geo-tagging) in your tweets, blogs, or social network accounts.
- Consider disabling location services altogether. Be aware, of course, that this will restrict such features as maps, bus route data, or services that allow you to watch over your children.
- Use location features selectively. For example, turn on geo-tagging of photos only when you need to mark them with your location. Remember that it is safer not to geo-tag photos of your children or your house.
- Share your location only with those you trust. Use privacy controls to restrict access to location status updates, messages, and photos.

Limit who knows your location

- Disable the option that allows others to share your location (check you in)
- Set your location data so that it's not publicly available or searchable
- If you use location services, check in thoughtfully
- Pay attention to where and when you check in
- Does it enhance or harm your reputation?
- Does it put others at risk? Are you alone? If so, is checking in safe?
- Link to social media with care. Avoid sending your check-ins to Twitter, Facebook, or your blog

Risks of failing to address risk in relation to safeguarding user safety

Risk to user
Could result in an increased risk of physical and or psychological harm to user(s). It could also pose a risk of a breach of confidentiality.

Financial and reputational risk
If a member of staff were to abuse their position of trust and duty of care their actions could put the provider at risk of legal action, loss or disruption of service provision and result in the loss of trust of the service by users

Table 3.0: Privacy and Safety: Risk Awareness and Management Programme to manage key risks in relation to Content

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Content	Risk of a user's personal/sensitive information becoming exposed to an unintended audience though their own actions, or those of other users or staff. Disclosure and/or exposure of personal sensitive information may result in adverse consequences – content disseminated online. If providing an anonymous service – consider the aforementioned risks.	Providers need to build in a range of privacy setting and provide clear and accessible supporting information. These resources will encourage users to make informed decisions about the information they post online. • Online mental well-being service providers operating a dedicated service should ensure that a user's personal and sensitive information is not searchable. • Users and staff should be provided with clear guidance about the prohibition of the use in the public domain of personal and sensitive information about other people gained in an online well-being context. • On 'satellite' presences, safety messaging and measures (eg, pre-moderate, post-moderate comments) should be put in place to ensure that users do not disclose personal/ sensitive information. • In the event of disclosure, clear policies and procedures re: handling disclosures needs to be developed. • Staff should be required to work within clear guidance that protects user anonymity and provides for systems and processes to protect a user who is at risk of being identified. • Users and staff should be provided with clear guidance about the prohibition of the use in the public domain of personal and sensitive information about other people gained in an online well-being context.	• Adhere to Internet safety related good practice guidelines developed by the Internet industry designed to enhance the safety of users. • Develop, implement and evaluate the efficacy of privacy settings and privacy and safety related policies and procedures. • Provide users with easy to understand safety and privacy guidance. • Solicit feedback from users about their levels of satisfaction with privacy and safety settings. • Ensure reporting systems are in place and respond to reports of misuse or inappropriate disclosure of personal sensitive information. • Develop training and guidelines for staff to ensure consistent safe practices. • Disciplinary system in place in the event that staff breach guidelines. • Published 'rules' of use of the service. • Systems for reviewing content and reacting to inappropriate content.	

Table 3.1: Privacy and Safety: Risk Awareness and Management Programme to manage key risks in relation to Contact, Conduct and Commerce

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Contact	Risk of cyber-stalking and online solicitation and harassment	• Users should have access to easy to use tools to report any inappropriate contact by or conduct from another user	• Policies and procedures in place to deal with reports of alleged cyber-stalking, bullying, harassment, defamation and online solicitation.	
Conduct	Failure to respect/ protect personal identity and information posted by other users	• Users should be confident in house rules of the service in the protection of their personal information and that of other users.	• Agreed house rules to reduce the risk of breach of confidentiality supported by on line education material for users and staff.	
Commerce	Commercial misuse of the information obtained by providers	• Users should be made aware - through a privacy policy and other means - of the extent to which information they place on the site will be shared for commercial purposes and used by the provider or third parties for market research.	• Use of information policy and procedures covering both internal and external use of data gathered about users by the provider. • Opt-out marketing options give users the choice of whether or not to receive special offers or telephone solicitations as a result of registering to use the online community.	

4. MODERATION

MODERATION

General guidance and resources

It is important for online well-being service providers to undertake a risk assessment of their own service and the potential for harm to children, young people and vulnerable adults in order to decide what safeguards to deploy, including the use of moderation.

Moderation and reporting pathways

Moderation is an activity or process following an agreed policy or set of guidelines to encourage safe and responsible use of an interactive service in accordance with the Terms of Service, Acceptable Use Policy or 'House Rules'.

Moderation is performed by human moderators or filtering software (or a combination) reviewing content posted by users and removing content or restricting users as necessary, either pre- or post-publication in near real time or following user reports.

UKCCIS has produced a set of Moderation Good Practice Guidance[18] that can be applied to user interactive services through which individuals can make contact and exchange content and personal information with other users in a virtual public "space", such as but not limited to:

- Forums/message boards including comments and reviews
- Blogs and micro blogging
- Social networking
- Massively Multi-Player Online Games (MMOG's or MMO's)
- Virtual worlds
- TV chat services
- Video sharing sites

It is important to consider developing, reviewing or updating polices on the recruitment, on the selection, training and supervision of moderators to safeguard against unsuitable individuals gaining contact with children; and reporting of incidents and concerns.

Children's Workforce Development Council (CWDC) has produced helpful guidance and online training on safer recruitment - "Recruiting safely: Safer recruitment guidance helping to keep children and young people safe" http://www.cwdcouncil.org.uk/. Where relevant, carry out the appropriate CRB or AccessNI (Enhanced Disclosure) and ISA registration check prior to an appointment to a position, paid or unpaid, where the duties involve a regulated activity involving moderation as set out in the Safeguarding Vulnerable Groups Act 2006 and the Safeguarding Vulnerable Groups (NI) Order 2007 – subject to the outcome of the ongoing review – and interview face-to-face all prospective volunteers and employees for moderation positions involving contact with children.

Reporting pathways

User reports to service provider

Online well-being service providers should provide easy-to-use mechanisms for users to report conduct or content that violates a well-being provider's Terms of Service, acceptable use policy and/or community guidelines. These mechanisms should be easily accessible to users at all times and the procedure should be easily understandable and age-appropriate.

- Reports should be acknowledged and acted upon expeditiously.
- Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled.

[18]Good practice guidance for the moderation of interactive services for children - http://media.education.gov.uk/assets/files/pdf/i/industry%20guidance%20%20%20moderation.pdf

Handling and escalating reports
Effective moderation also requires a clear reporting policy that identifies reporting pathways and associated protocols and procedures with respect to how the well-being provider handles a variety of situations including risk to life:

- The reporting policy should provide moderators with clear guidance about what to do, who to escalate reports to, when and how. The policy should also cover situations where the moderator observes behaviour that gives cause for concern on the service and involves escalation to a moderator's supervisor, manager or abuse management team.
- The reporting policy should address what moderators should do when potential illegal images of children are identified. This should include the handling, storage and reporting of potential illegal child abuse images to the appropriate authority. In the UK this is the IWF or the police, in accordance with the Sexual Offences Act 2003 and the accompanying Memorandum of Understanding – further information on the MOU is available on the CPS website, www.cps.gov.ukand the IWF website www.iwf.org.uk
- Each organisation's reporting policy should define what 'urgent and serious' incidents are, and to define their procedures accordingly. In instances where it is deemed appropriate, the policy should include details of how to contact the appropriate child protection and law enforcement agencies. The policy should list clear procedures for the disclosure of data and other non-public information to law enforcement agencies, which are compliant with relevant data protection and privacy laws.
- Have in place clear procedures to allow for the disclosure of communication data and authenticating communication data requests from public authorities in accordance with relevant legislation, Regulation of Investigatory Powers Act[19] (RIPA, 2000).

These procedures may include:

- What communication data can be disclosed and to which public authorities.
- Authenticating a request from a public authority to disclose data.
- A designated person or contact point for the purpose of liaising with public authorities, including law enforcement, and
- A record of disclosures made to public authorities.

Risk of not having effective procedures in place

Financial and reputational costs
In English tort law another person or an organisation may owe an individual a duty of care, which involves ensuring that the individual does not suffer an unreasonable harm or loss. If such a duty of care is breached and harm occurs as a direct result of that breach then a legal liability is imposed upon the duty-ower to compensate the victim for any losses they incur.

From a user's perspective
Users will have a reasonable expectation of the well-being provider's duty of care with respect to the user's well-being. A breach in duty of care or negligence on behalf of the well-being provider may have a number of negative consequences for users, including exposure to inappropriate or illegal content, contact or conduct.

[19]For further information about RIPA 2000 see www.legislation.gov.uk and www.homeoffice.gov.uk

Table 4.0: Moderation and reporting pathways: Risk Awareness and Management Programme to manage key risks in relation to Content and Contact

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Content	Risk of a user's personal/sensitive information becoming exposed to an unintended audience	Clarity regarding: • The Terms of Service of the provider and • What constitutes a potential legal breach of the terms of Service	• Explicit Terms of Service which set boundaries for responsibilities and explicitly define the groups of persons for which the service has a 'duty of care' • If relevant written details of how this operates if the service is provided wholly in a anonymised format *Note: It is important to note the general principle that an action that is illegal if committed offline is also illegal if it is committed through an interactive service. This applies to issues such as distributing illegal material. Clear reporting mechanisms and policies for handling reports are essential.*	
Contact	Harmful behaviour e.g. harassment or grooming Inciting someone to commit an offence via the provider website Fraud and identity theft	• Clear user 'house rules' • Effective reporting and investigation systems for all alleged breaches of house rules • Evidence that changes have occurred as a result of investigation	• Simple mechanism for users to report incidents • Incident reporting and investigation processes	

Table 4.1: Moderation and reporting pathways: Risk Awareness and Management Programme to manage key risks in relation to Conduct and Commerce

Risks	What are the key risks to be addressed?	What safeguards will users need to be confident that risks are mitigated to an acceptable level?	What systems and processes are required to make this happen?	✓
Conduct	Risk of harm to vulnerable users	Effective safeguarding principles upheld by provider in a way that is visible to user	• Safeguarding Policies and Procedures for children and vulnerable adults • Agreed effective reporting mechanisms with e.g. police, social services, other statutory agencies • Investigation procedures for incidents • Links via website to other approved agencies that can offer support to individual users experiencing difficulties	
Commerce	Harm caused directly or indirectly to a user from exposure to advertising on the site	Limited safe supported advertising	• If commercial advertising is to appear on the site, adherence to the Advertising Standards CAP code is essential. • Conduct a risk assessment to ascertain the effectiveness of advertising 'neutral' and at best enhance the well-being of the user	

APPENDIX

Appendix:

The **RAMP** complements existing good practice guidelines and ethical frameworks, - some of which are listed below. These have been developed by policy groups that were acting independently, but which collectively serve to shape a consistent and complementary framework. Mental well-being providers can utilise this framework to build and develop strategies to support and protect service users online.

The British Association for Counselling & Psychotherapy (BACP) is a membership organisation and a registered charity that sets standards for therapeutic practice and provides information for therapists, clients of therapy, and the general public. As the largest professional body representing counselling and psychotherapy in the UK, BACP aim to increase public understanding of the benefits of counselling and psychotherapy, raise awareness of what can be expected from the process of therapy and promote education and/or training for counsellors and psychotherapists. BACP has created a document that outlines the Ethical principles of counselling and psychotherapy[20]

The Online Therapy Institute has developed an international self-regulatory Ethical Framework, entitled Ethical Framework for the Use of Social Media by Mental Health Professionals, see http://www.onlinetherapyinstitute.com/ethical-framework-for-the-use-of-social-media-by-mental-health-professionals/

The UK Council for Child Internet Safety (UKCCIS) has developed a series of good practice guidelines that provide a useful starting point when considering designing services with interactive features aimed at young people and vulnerable adults:

- Good practice guidance for the providers of chat services, instant messaging (IM) and internet connectivity content and hosting.
- Good practice guidance for the moderation of interactive services for children.
- EU self-regulatory initiatives[21] such as the Safer Social Networking Principles provide an excellent resource in terms of illustration of how various companies have implemented good practice principles.

Vodafone has developed a number of useful resources that mental well-being providers should review including:

- A website for parents to help them engage with their children's digital worlds, including well-being issues, for example online bullying and self harm issues - www.vodafone.com/parents. **Digital Parenting Magazine** – a Digital Magazine with information supporting parents and carers engage with children's digital worlds
- **Vodafone Digital Parenting App** – an App for Android mobiles with key highlights from the Digital Parenting Magazine – can be downloaded from the Digital Parenting website www.vodafone.com/parents
- **Vodafone Guardian App** – an App for parents to safe guard their children's use of Android Mobile phones managing their access to the Internet, time limits for usage and tools to manage the camera and Blue Tooth functions. Downloadable from www.vodafone.com/parents

Facebook: Mental well-being organisations wishing to develop a social media marketing strategy should refer to Facebook's marketing resource for not-for-profits - http://www.facebook.com/nonprofitmarketingguide?sk=wall.

Facebook has developed a comprehensive set of Internet safety education resources – see https://www.facebook.com/safety

Mental well-being service providers who are considering the delivery of part of their service via mobile phones should be aware of the European Framework for Safer Mobile Use by Younger Teenagers and Children[22]

- For insights into how mobile operators have implemented the Framework, service providers should visit http://www.gsmeurope.org/safer_mobile/implementation.htm.

Mental well-being providers should also be aware of a recent set of mobile privacy guidelines for publishers that advises that privacy policies should explicitly state what information, including location and the Unique User ID (UUID), is being captured, paired with other data and/or shared with third parties. It is important to keep up to date on regulatory changes that can impact on the services you offer online. If you offer a service that is monetised through advertising you should note that users ought to be allowed to opt-out of behavioural targeting of mobile ads.

[20]Ethical principles of counselling and psychotherapy - http://www.bacp.co.uk/ethical_framework/ethics.php

[21]Implementation of the Safer Social Networking Principles for the EU http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip/index_en.htm

[22]European Framework for Safer Mobile Use by Younger Teenagers and Children http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf

Applications: Mental well-being providers may also wish to use applications to deliver one or more aspect of a service and should be aware of a set of good practices with respect to user privacy designed for application developers:

The Centre for Disease Control and Prevention has developed The Health Communicator's Social Media Toolkit[24] and to access examples of social media policies see: http://socialmediagovernance.com/policies.php

Samaritans Workplace Training team provides in-house training services to external organisations, such as online moderators, in UK & ROI based on nearly 60 years of experience in supporting those in emotional distress. Samaritans has identified that although employees feel sufficiently trained in practical work areas the majority of employees can feel inadequately prepared for emotionally challenging situations including handling distressed customers and staff members. Samaritans courses do not seek to turn staff into counsellors or Samaritans, they are focused on sharing our simple and effective tools and techniques designed to equip employees with the skills and confidence to handle angry, aggressive, distressed or vulnerable customers in an effective, sensitive and professional way.

For more information about Samaritans training services please contact externaltraining@samaritans.org or visit

http://www.samaritans.org/your_emotional_health/workplace_training.aspx.

Guidance for Commissioning IAPT Training 2011/12[25] On 2 February 2011, the Government published No Health without Mental Health, which sets out the strategy for improving the mental health and well-being of the nation. Central to this strategy is the Government's commitment that the NHS will complete nationwide roll-out of Improving Access to Psychological Therapies (IAPT) services between 2011/12 and 2014/15.

Design by Vivid Lime (www.vividlime.com)

[23]http://www.mediapost.com/blogs/raw/?p=6837

[24]The Centers for Disease Control and Prevention, has developed The Health Communicator's Social Media Toolkit http://www.cdc.gov/healthcommunication/ToolsTemplates/SocialMediaToolkit_BM.pdf

[25]Guidance for Commissioning IAPT Training 2011/12 https://docs.google.com/viewer?url=http%3A%2F%2Fiapt.nmhdu.org.uk%2Fsilo%2Ffiles%2Fguidance-for-commissioning-iapt-training-201112-201415.pdf

DELIVERING MENTAL WELL-BEING SERVICES ONLINE

A guide to the provision of safe and secure mental health and social support services online. A RAMP Initiative.

DRIVERS

- Increases in internet use and health related search
- Proliferation of unregulated unreliable/dangerous advice websites
- Patient desire for discretion and anonymity
- Government encouragement to use digital
- Cost savings from online delivery of care

BENEFITS

- Increased accessibility
- De-Stigmatisation
- Choice
- Dilution of risk
- Meets strategic goals of the Department of Health

GETTING STARTED WITH NEEDS ANALYSIS

- Define the purpose of your online presence and interaction, e.g.
  - signposting, information provision, awareness/fund raising, counselling, community building
- Online channel selection/mix
- Staff training

ONLINE SERVICE TYPES

- Knowledge, answers and advice
- Peer to peer mentoring
- Online Computerised Cognitive Behavioural Therapy
- Counselling/psychological intervention

ramp

Risk Awareness and Management Programme

RAMP is a framework and programme designed to help organisations operate online interactive services more responsibly and safely with the wellbeing of their users in mind.

RAMP QUESTIONS

- What are the risks to an end user and a provider associated with the well-being of users of interactive services?
- What safeguards can be put in place to ensure confidence about the service?
- What safety measures, system and processes are needed to make this happen?

RAMP AREAS

- Organisational Data Protection
- End-user Privacy and Safety
- Informed Consent
- Moderation and Reporting Pathways

CATEGORIES OF RISK

- Content risks
- Contact risks
- Conduct risks
- Commercial risks

RAMP ACTIONS

- Terminate
- Tolerate
- Treat
- Transfer

SPONSORS

facebook

The Tavistock and Portman NHS
NHS Foundation Trust

bacp
British Association for Counselling & Psychotherapy

vodafone

www.facebook.com/rampguide

info@rampguide.net