**eResponse Group**

**e-Safety Policy**

Version 1 - December 2015

**Introduction**

eResponse recognises the benefits and opportunities which new technologies offer to teaching, learning and assessment delivery and practice. At eResponse, we encourage the use of a wide range of technology wherever possible in order to enhance learners' skill development, knowledge, understanding, application to independent work and research and to promote achievement and success. However, the generally highly accessible and global nature of the internet, access and the wide variety of technologies available does impact on risk and large range of potential risks and challenges associated with such use for all parties and users concerned.

eResponse policy and approach is to implement safeguarding practice that meets not only with legislative requirements but also with the organisations values and practice to safeguard all learners and staff, providing regular training, updates and raising awareness of legal and safe practice requirements. We strive to ensure safe use by learners when on site with restricted access to websites through threat detection and internet blocking systems, which monitor learner use.

Through robust risk assessment management, we assess learning environments according to location. As an organisation, through the safeguarding learners' national legislation, we adopt a high standard of duty of care and health and safety including stay e-safe and secure when using internet sites and publications. This e-safety policy should be read in conjunction with other relevant policies: Safeguarding, Email and Internet usage, Harassment and Bullying.
e-Safety Risks
This policy identifies the risks which can be summarised under the following headings, as identified in Becta’s Safeguarding Children in a Digital World advice. This policy also details the strategies involved in minimising the e-Safety risks.

- Examples of E-Safety Content
- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse
- Examples of E-Safety Contact
- Grooming using communication technologies, leading to sexual assault and/or child prostitution
- Examples of E-Safety Commerce
- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams
- Examples of E-Safety Culture
- Bullying via websites, mobile phones or other forms of communication devices
- Downloading of copyrighted materials, e.g. music and films

eResponse Safeguarding Group is represented by members of the leadership team and trained safeguarding specialist staff as detailed in the Safeguarding Policy. The impact of the policy will be monitored regularly with a full review being carried annually. This policy will also be reconsidered where concerns are raised by leadership, safeguarding officers or any learner or member of staff where an e-safety incident has occurred. All incidents will be dealt with quickly and records completed with swift intervention to protect the individual/s concerned.

Policy Scope
The policy applies to all members of eResponse community who have access to the organisations IT systems, both on the premises via remote use. Any user of eResponse IT systems must adhere to the e-Safety Rules and the E-Mail and Internet Usage policy. The e-Safety Policy applies to all use of the internet and electronic communication devices, i.e. e-mail, mobile phones, games, consoles, social networking sites, and any other systems that use the internet for connection and providing of information.
Roles and Responsibilities
There are clear lines of responsibility for e-safety within eResponse. The first point of contact should be one of the Safeguarding Officers. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved unless learners are under the age of eighteen years of age where special consideration is adhered to.
All learners must know what to do if they have e-safety concerns and who to talk to. Where any report of an e-safety incident is made; all parties must know the detail of the procedure and processes for follow up. Where the leadership and safeguarding team considers it appropriate, the allocated officer may be asked to intervene with swift and appropriate additional support from external agencies where needs are identified.

Security
eResponse will do all that it can to make sure that the organisations IT network, facilities and sites are completely safe and secure. Regular checks on technology equipment are undertaken to maintain the latest versions of security software. Effective security measures will include the use of enhanced filtering and protection of appropriate firewalls, servers, routers, workstations etc. to prevent accidental or malicious access of systems and information. Digital communications, including email and internet postings will be monitored in line with the Network Usage Policy.

Behaviour
eResponse will ensure that all users of technologies adhere to the standard of behaviour as set out in the E-mail and Internet Usage Policy. eResponse will not tolerate any abuse of IT systems, whether online or offline. All communications by learners and staff should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the learner and staff disciplinary policies and procedures. Where conduct is found to be unacceptable, eResponse will initiate the compliance procedure and disciplinary action will be taken including reporting the incident and full details including names of those involved to the police if the situation that has occurred is deemed illegal.

Use of Images and Video
The use of images and photographs are often effectively used in teaching, learning and assessment practice and are encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to learners or staff. All learners and staff receive training on the risks in downloading these images as well as posting them online and sharing them with other colleagues. There are particular risks where personal images are posted onto social networking sites and these risks are highlighted during safeguarding training.
Personal Information

eResponse collates and files personal information of learners and staff regularly in confidential files held in the HR department. This information is stored in accordance with the current relevant Data Protection Act guidelines. Staff are fully aware that learners’ personal information must be stored safely and securely at all times. When using an online VLE platform, all personal information must be password protected. Under no circumstances are any individual’s personal information taken off-site. All personal information must be stored on the centralised MIS system and password protected.

Teaching, Learning and Risks Assessment

With the current unlimited nature of internet access, it is virtually impossible for eResponse as an organisation in workplace learning with inclusion of a wide ranging cohort of learners that all potential risks can be eliminated for learners and staff. Risk assessments are undertaken by management, tutors and assessors both on site and in the workplace environments. Reports and action plans are completed where areas requiring improvement need to be addressed.

Incidents and Response

Where an e-safety incident is reported to eResponse staff, this matter will be dealt with immediately and with swift intervention. A member of the leadership team will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to any member of staff within eResponse, to one of the safeguarding officers or to the leadership team direct who adopt an open door policy.

Where a member of staff wishes to report an incident, they must contact their line manager. Following any incident, eResponse will review the incident and history, deciding on the most appropriate quick intervention and course of action. Sanctions may be put in place immediately if the incident is deemed to be more serious and external agencies involved or the matter may be resolved internally dependent on the seriousness of the situation. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies and potentially the policing authorities and child protection agencies.

Policy approved by:

Barbara Van der Eecken – Director of Quality and Standards

Date Updated: 14/12/15
Date for Review: December 2016