

**DIGITAL AND E-SAFETY POLICY**

**Date: 1 October 2017**

**Review date:1 October 2018**

**Statement of Purpose**

Omega Care Group acknowledges that digital technology is an embedded element within all our lives and that it offers a wide range of positive benefits.

As an organisation, we seek to guide and support young people in their appropriate use of technologies, in order to maintain their personal safety and of those they interact with.

Omega Care Group recognises that risk cannot be entirely eliminated, and aims to equip young people with the skills, knowledge and resilience to best empower them in the maintenance of their safety in a digital world. This position is supported by effective working practices, and robust recording and reporting procedures and an appropriately trained and aware staff team.

Omega Care Group takes the position that digital and e-safety is a safeguarding concern, with the technologies providing the means for the child protection issue to develop.

**Means of Achievement**

To meet the Statement of Purpose and its objectives, Omega Care Group will:

1. Provide online safety training for all staff within the induction process.
2. Actively promote a culture of digital/e-safety awareness.
3. Promote responsible, knowledge based decision making.
4. Address digital/e-safety through the Independent Living Programme and key work sessions.
5. Ensure transparency and open lines of communication.
6. Operate within professional boundaries.
7. Manage and evaluate risk factors including emerging technologies.
8. Promote the acquisition of self risk management skills.
9. Ensure robust recording and reporting procedures are in place.
10. Operate a signed Acceptable Use Policy for all staff, with clear parameters.
11. Operate within clear guidelines for cyber-bullying.
12. Ensure confidentiality and data protection issues are addressed.
13. Provide access to resources to promote awareness and best practice.
14. Ensure young people are aware of their rights and responsibilities.
15. Provide oversight on Digital/e-safety issues through the Safeguarding officer.
16. Operate an effective filter on broadband access within each unit.
17. Provide information and support regarding privacy settings on social media.
18. Review this policy annually or as appropriate in light of any significant development in use of technology and/ or an incident taking place.

**Supporting/Relevant Legislation**

1. Equality Act 2010
2. Protection from Harassment Act 1997
3. Communications Act 2000
4. Computer Misuse act 1990
5. Criminal Justice and Courts Act 2015
6. Protection of Children Act 1978
7. Criminal Justice Act 1988
8. Data Protection Act 1998
9. Racial and Religious Hatred Act 2006
10. Serious crime Act 2015

**Role of Safeguarding Officer**

The Safeguarding Officer will be trained in online/digital safety, and coordinate appropriate training for the whole staff team. The post holder will receive and oversee all reports and incidents and act as a liaison with the LCSB and the police where appropriate.

The Safeguarding Officer will have a particular awareness of risk involved in:

1. Sharing of personal data
2. Access to illegal/inappropriate images
3. Inappropriate online contact with adults/strangers
4. Potential or actual incidents of grooming
5. Cyberbullying.

**Young People and Potential Risks**

**Content:**

In this context, the young person is the recipient of material. The young person is exposed to material which can include illegal, harmful or inappropriate images or other content.

Examples include:

1. Extreme violence
2. Pornography
3. Hate based materials
4. Material promoting extremist ideologies
5. Criminally racist material

**Contact:**

In this context, the young person is a participant/victim, and is subjected to harmful online interaction. This can include:

1. Harassment/stalking
2. Being groomed for sexual abuse on meeting strangers
3. Being groomed through extremist ideologies

**Conduct:**

In this context the young person is a perpetrator, a victim or both. This is personal online behaviour that increases the likelihood of, or causes harm. This can include:

1. Cyber bullying
2. Hostile/aggressive peer activity
3. Sexual harassment, ‘sexting’-sending/receiving personally intimate images
4. Hate crimes
5. Potentially harmful user generated content e.g. providing advice/support for promoting eating disorders
6. Privacy issues, including the disclosure of personal information.

**Commercial:**

In this context the young person is a participant/victim. This can include:

1. Gambling
2. Paid for, on line gaming
3. Buying/selling goods on line.

**Digital Images: taking and distribution**

**Young People**

Young people will be made aware of the risks associated with taking and publically sharing and distributing images. This will take place during Key Work sessions as part of the Independent Living Programme. Issues addressed include loss of control of the content, possible impacts and the potential for criminal offence if the images are sexual in nature. Young people will be made aware of the dangers to themselves and others of posting images which enable the identification of a location.

**Staff**

Images of young people may only be taken on Omega Care Group owned equipment. Such images may only be used internally e.g. within the individual Portfolio of Achievement, and require written permission from the young person and their social worker. All images must be appropriate in nature, identified only by first name, collected in a professional way and logged. Downloading should be carried out within 3 days and the date of downloading logged. Logs and memory cards will be monitored. Under **no** circumstances should staff use their personal devices to collect images of young people.

**Safe Practice: Young People**

Young people will be informed and supported to:

1. Access age appropriate material on the internet-with a filter on the company broadband.
2. Make best use of privacy settings, including blocking specific contacts, on all social media, and to understand the importance and relevance of this.
3. Understand confidentiality and the importance of not sharing personal information on line-name, address, age, places they frequent etc.
4. Use the internet safely and appropriately, and to understand what they should do and whom to speak with if they are upset or disturbed by what they see, or by what has been communicated to them. Young people should be made aware of reporting mechanisms, and of how to access support through specialist organisations.
5. Understand that the private buying and selling of goods online **may not** be carried out from the unit, and of the reasons for this-maintaining safety and security of all in the house.
6. Use age appropriate computer/console games only, in communal spaces within the unit-any game that is classified as an 18 should be used only in the individual’s room.
7. Understand what is acceptable and unacceptable digital online behaviour, and to act in a personally responsible way.
8. Respond appropriately to issues of Cyber-Bullying.

**Safe Practice: Staff**

1. Staff should not share personal information with young people, this includes e-mail addresses, phone numbers and social media access.
2. **All** contact with young people should use **only** Omega Care Group equipment and should be professional in nature, this includes any contact by e-mail, phone or social media.
3. Staff should pay due regard to confidentiality and the Data Protection Act and ensure that no information is disclosed which could constitute a breach. This includes their own privacy, that of colleagues and of young people.
4. Staff must comply with the Professional Boundaries protocols.
5. Staff will undertake digital/e-safety training and ensure currency, and ensure effective recording and reporting.
6. Staff should not use personal devices to record digital images.
7. Staff are required to sign and commit to, the Acceptable Use Policy.

**Staff Personal Devices**

Staff may use their personal mobile phones whilst at work, but should ensure that this is not in the presence of young people, use is kept to a minimum and that due professionality is maintained. Staff are responsible for maintaining the security of their device, and of ensuring that young people remain unaware of the phone number.

If staff access the internet through a personally owned device (e.g. a tablet) whilst on shift, they should ensure that said usage reflects the ethos of the organisation and complies with the Acceptable Use Policy. Such access should be confined to the office (i.e. away from the presence of young people) and should be minimised. Staff should ensure the security of personal devices at all times.

**Cyber-Bullying**

Cyber (online) bullying can be defined as:

‘the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else’.

Cyber-bullying is often linked to discrimination which may be: sexist, racist, faith based or connected to sexual orientation, gender identity or disability. Cyber-bullying impacts negatively on the individual’s sense of self worth and confidence, and can affect mental health and wellbeing.

Cyber-bullying can include: threats, intimidation, harassment, stalking, impersonation, public posting of private information/images and manipulation.

**Response:**

1. Follow **disclosure** protocols (ref: Safeguarding Policy) when taking a report from a young person.
2. Safeguarding officer to be notified immediately on report or identification of incident.
3. Digital/e-safety incident report form to be completed (after support of young person)
4. Appropriate support to be offered to the young person and the spread of the incident contained.
5. Any evidence should be retained if possible, and the young person encouraged to assist in any investigation.
6. Social Care to be informed and updated.

The young person should be advised not to reply or retaliate. Advice should be given about blocking any further communication.

If the Cyber-Bullying involves illegal content or activity including:

1. Indecent images of a young person under 18
2. Obscene content (e.g. torture, rape)
3. Hate crimes including racist and homophobic threats
4. Threats of violence
5. Rape or death threats
6. Stalking or harassment.

Then the young person should be considered as being at **immediate risk** and police engagement sought immediately.

(Ref: Omega Care Group Anti-Bullying policy)

**‘Sexting’**

The sending or receiving of personally intimate images.

If a sexting incident occurs/comes to the attention of staff should:

1. Report to the Safeguarding Officer immediately.
2. **Never** view, download or share the imagery or ask the young person to do so-this is **illegal.** If viewed by accident, before being able to inform the young person not to show it to them, the SO **must** be informed.
3. Not delete the imagery or ask the young person to do so.
4. Not ask the young person to disclose information regarding the imagery-this is the responsibility of the SO.
5. Not share information about the incident to other staff members or young people who may be involved.
6. Not say or do anything to blame or shame any young person involved.
7. Explain the need to report the incident and to ensure the safety of the individual.
8. Provide appropriate person centred support.

(Ref: Omega Care Safeguarding policy)

**Acceptable Use Policy - Staff**

This identifies the parameters of safe digital and internet use, and outlines the responsibilities of staff to ensure that they act appropriately, maintain personal safety and that of, and comply with best practice directives. All staff are required to agree to and operate within this framework and sign the attached signing sheet to agree to the following:

1. I will immediately report any illegal, harmful or inappropriate material or incident to the Safeguarding Officer.
2. I will only communicate with young people using official Omega Care Group systems-phone-e-mail-social media.
3. I will not use my personal devices to record images.
4. I will not engage in any on line activity that may compromise my professional reputation.
5. I will not try to access/upload or download any materials which are illegal. This includes Child Sexual abuse images, criminally racist materials, adult pornography covered by the Obscene Publications Act and inappropriate material which may cause harm to others.
6. I will not try to use any resources to enable the broadband filter system to be bypassed.
7. I understand that the Data Protection Act requires staff and young people’s data – to which I have access to be privileged and confidential. The exception to this is when deemed necessary by law/policy to disclose such information to the appropriate authorities.
8. I understand that this Policy applies to my use of personal devices at work, or in situations related to my employment by the organisation.
9. I will not attempt to install soft/hard ware without appropriate permissions.
10. I will promote digital and e-safety with young people and support the development of safe and responsible interactions.
11. I understand that the information systems are the property of Omega Care, and that it is a criminal offence to use a computer for a purpose not permitted by the organisation.
12. I understand my responsibilities in accessing training and retaining currency in digital and e-safety.
13. I will maintain the security of my own digital devices whilst at work and use them appropriately.
14. I will ensure all my work is compatible with the Professional Boundaries protocols.
15. I will not share any personal information with young people including: phone number, e-mail address, social network access or gaming ‘tag’.

I have read, understood and agree to use Omega Care Group digital technology, both on and off site, and my own devices- on site and when work related within these guidelines.

I understand that this framework may evolve and that I will be informed of any developments.

I understand that I may be subject to the organisation’s disciplinary procedures should I fail to adhere to the above Policy.