DIGITAL AND E-SAFETY POLICY

1. **Scope**
   1. This policy shall apply to all employees of Omega Care Group including full time staff, part time staff, temporary staff and bank staff.
   2. The policy outlines operational practice to create a positive environment where children and young people can live and flourish.
   3. This policy is applicable to all services operated by Omega Care Group.
2. **Objective**
   1. 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 with the possibility of opening up new opportunities for everyone.
   2. Omega Care Group recognises that all risk cannot be eliminated and aims to equip both employees and children & 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 procedures and an appropriately trained and aware staff team.
   3. As an organisation, we seek to guide and support both our employees and children & young people in their appropriate use of technologies, in order to maintain personal safety and the safety of those they interact with. This policy aims to give staff clear guidance regarding digital e-safety.
   4. 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.
3. **Means of Achievement**

To meet the objectives, Omega Care Group will:

* Provide on-line safety training
* Actively promote a culture of digital/e-safety awareness.
* Address digital/e-safety through the Independent Living Programme.
* Ensure transparency and open lines of communication.
* Operate within Omega Care’s Professional Boundaries Policy.
* Manage and evaluate risk factors including emerging technologies.
* Promote the acquisition of self-risk management skills.
* Ensure robust recording and reporting procedures are in place.
* Operate within clear guidelines for cyber-bullying.
* Ensure confidentiality and data protection issues are addressed.
* Provide access to resources to promote awareness and best practice.
* Ensure young people are aware of their rights and responsibilities.
* Provide oversight on digital/e-safety issues through the Designated Safeguarding Officer.
* Operate an effective filter on broadband access within each home to protect Children and Young People.
* Provide information and support regarding privacy settings on social media.
* Review this policy annually or as appropriate in light of any significant development in use of technology and/or incident taking place.

1. Children and Young People internet usage and activity is monitored by the child’s staff team. All internet arrangements are agreed by the home manager and Social Worker. This is outlined within the child and young person Residential Care Plan.
2. **Potential Risks to Children & Young People**

* Access to illegal, harmful or inappropriate images or other content.
* Loss of privacy/control over personal information.
* Grooming by those who may be able to make contact with them.
* The sharing/distribution of personal images without their consent or knowledge.
* Inappropriate communication/contact with others, including strangers.
* Potentially harmful user generated content e.g. providing advice/support for promoting eating disorders.
* Cyber-bullying
* Digital, Gaming and Social Media Addictions
* Access to unsuitable images, videos, internet games.
* Plagiarism and copyright infringement.
* Illegal downloading of music and/or video files.
* Hacking, viruses and system security.
* The potential for excessive use which may impact on the social and emotional development and the learning of the young person.
* Gambling
* Online gaming at a cost.
* Buying/selling goods online.
* Hate based materials/racist material

1. **Role of Designated Safeguarding Officer**
   1. The Designated 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 Safeguarding Partners and the police if necessary.
   2. The Designated Safeguarding Officer will have awareness regarding all of the above and will be the point of contact within Omega Care Group.
2. **Digital Images: Taking and Distributing**
   1. Children and Young People
      1. Young people should be made aware of the risks associated with taking and sharing images including video and photography. Issues addressed with the child & young person should cover loss of control of the content, possible impacts and the potential for criminal offence if the images are inappropriate.
      2. If a child is unsure of the nature of photographs or videos, they should be aware they should seek approval from an appropriate staff member. Child / Young people should be made aware of the dangers to themselves and others posting images which enable the identification of a location.
   2. Staff
      1. Staff should ensure images of Children and Young People are only taken on equipment owned by Omega Care Group for the purposes of Omega Care Group. Such images will only be used internally for example; within the progression file and memory books.
      2. Staff are required to obtain written consent from the young person prior to taking and using such images. This is obtained within the child’s admission process.
      3. 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 should be logged appropriately.
      4. Under NO circumstances should staff use their personal device to collect images of young people. In doing so may result in disciplinary action. Staff must also not allow the young person to take images of them for their own personal use. All children must consent to having their photographs or any digital images
      5. If a member of staff suspect a child is at risk, a risk management plan must be completed for the individual child.
3. **Safe Practice**
   1. **Children and Young People**

Children Young people will be informed and supported to:

* Access age appropriate material on the internet, with a filter on the company broadband.
* Make best use of privacy settings, including blocking specific contacts, on all social media, and to understand the importance and relevance of this.
* Understand confidentiality and the importance of not sharing personal information online.
* Use the internet safely and appropriately and to understand what they should do and who they should refer to should they come across inappropriate material.
* Understand that private buying and selling of goods online must NOT be carried out from the unit. The reasons for this is to maintain the security of all in the house.
* Use age appropriate computer/console games only, in communal areas within the home.
* Understand what is acceptable regarding digital online behaviour.
* Make staff aware of any issues of cyber-bullying.
  1. **Staff**
     1. Staff should not share personal information with young people, this includes passwords, e-mail addresses, phone numbers and social media access.
     2. All contact with young people should only be via Omega Care Group equipment and should be in a professional nature this includes any contact by email or phone. Staff must not accept friend requests from children or young people on social media.
     3. Staff must liaise with the assigned Social Worker at the start of the placement regarding internet usage and the child/young Person having access to the internet. The home manager is accountable in ensuring this task is completed.
     4. Staff must not post anything on social media that may be interpreted as slanderous towards colleagues, children/ young people or Omega Care Group as a business.
     5. Staff should ensure confidentiality at all times and adhere to the Data Protection Act ensuring information disclosed is not in breach of these guidelines.
     6. Staff must comply with the Professional Boundaries Protocols.
     7. Staff must undertake digital/e-safety training as and when required. They must ensure effective recording and reporting.
     8. Staff must not use their own personal devices within the home or during their shift.
     9. All staff must read and sign the acceptable use policy

1. **Staff Personal Devices**
   1. Staff must not use their personal mobile phone or any other personal device (e.g. laptops, tablets, memory cards) during works time. All devices must be switched off or turned on to silent and secured in a safe place out of view during their shift. Staff must also disconnect any smart watches from their personal devices during their shift.
   2. Staff must not bring fire sticks or any other TV streaming devices into the homes. They must not share Netflix account details or any other means which would allow the Child/ Young People to access any other channels that the ones authorised by Omega Care Group.
   3. Omega Care Group do not take responsibility for any personal property of staff while on shift. All personal property must be kept secure and not left out in view. Staff must take responsibility for all their own possessions.
   4. Staff must not access the internet for their own personal use. All internet access must be business related and must adhere to the rules set out in Omega Care Group’s policies and procedures.
   5. All staff must sign the acceptable use policy
2. **Cyber-bullying**
   1. 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.
   2. Cyber-bullying can also include threats, intimidation, harassment, stalking, impersonation, public posting of private information/images and manipulation.
   3. Staff must:

* Follow disclosure protocols (ref: Safeguarding Policy) when taking a report from a Child/ Young Person.
* The Safeguarding Officer must be notified immediately on report or identification of an incident and carry out a risk assessment.
* Digital/e-safety incident report form to be completed (after support of the Young Person)
* Appropriate support to be offered to the Child/Young Person and the spread of the incident contained.
* Any evidence should be retained if possible, and the Child/Young Person encouraged to assist in any investigation.
* Social Care to be informed and updated.
  1. The Young Person should be advised to not reply or retaliate. Advice should be given about blocking any further communication.
  2. If the cyber-bullying involved illegal content or activity including:
* Indecent images of a young person under the age of 18.
* Obscene content (e.g. torture, rape)
* Hate crimes including racist and homophobic threats
* Threats of violence
* Rape or death threats
* Stalking or harassment

**Then the child should be considered as being at immediate risk and police engagement should be sought immediately. Please refer to Omega Care Group Anti-Bullying Policy.**

1. **Sexting**
   1. Sexting is the sending and/or receiving of personally intimate images. If a sexting incident occurs or staff suspect it may be occurring, then they should:

* Report it to the Safeguarding Officer immediately and carry out a risk assessment.
* Never view, download, or share the imagery or ask the young person to do so as this is illegal. If viewed by accident, then the Designated Safeguarding Officer must be informed of this.
* Do not delete the images or ask the Child/Young Person to do so.
* Do not store the image – this is illegal
* Do not ask the Child/Young Person to disclose information regarding the imagery, this is the responsibility of the Designated Safeguarding Officer.
* Do not share the information with other members of staff or other Children/ Young People.
* Do not do or say anything to suggest blame or shame on the Child/Young Person involved.
* Explain clearly to the Child/Young Person the need to report the incident and to ensure the safety of the individual(s) involved.

**Please refer to Omega Care Group Child Protection and Safeguarding Policy**

1. **Security and Confidentiality**
   1. Any concerns about the security of the ICT system should be raised to a member of the management team.
   2. Staff are required to keep any passwords confidential.
   3. Should a staff member be required to download materials they should ensure these materials are appropriate and only for the use of the business. Staff should take advice if they are unsure. Staff must also take responsibility if they are to share the materials with the young people that they are appropriate.
2. **Acceptable Use Policy**

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 the company, 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 and carry out a risk assessment.
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 online 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/hardware 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.