Online Safety

POLICY

Last Updated: 24/07/2019

Policy statement : We take steps to ensure that there are effective procedures in place to protect children, and young people from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting. Designated Safeguarding Lead (DSL) and the centre manager is responsible for ensuring that all IT equipment is safe and fit for use.

Procedures

Information Communication Technology (ICT) equipment

▪ Only ICT equipment belonging to the REACH is used by staff and students.

▪ The Centre Manager and DSL responsible for ensuring all ICT equipment is safe and fit for purpose.

▪ All computers have virus protection installed.

▪ Safety settings are checked to ensure that inappropriate material cannot be accessed.

Internet access

▪ Students do not normally have access to the internet and if they do it is never unsupervised access.

▪ If staff access the internet with students for the purposes of promoting their learning, written permission is gained from the person commissioning our services who are shown this policy.

▪ The centre manager has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.

▪ Students are taught the following stay safe principles in an age appropriate way prior to using the internet;

- Only go on line when supported by a member of REACH
- Be kind online
- Keep information about yourself safe
- Only follow links that you know are safe
- Tell a member of the REACH team if something makes me unhappy on the internet

▪ REACH staff will also seek to build children's and vulnerable adults resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure.

▪ All computers for use by students are located in an area clearly visible to staff.

▪ Students are not allowed to access social networking sites.

▪ REACH staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
▪ Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
▪ The Centre manager ensures staff have access to resources to enable them to assist students to use the internet safely.
▪ If staff become aware that a child is the victim of cyber-bullying, they pass the information to the DSL who will deal with the situation in line with our child protection and safeguarding procedures and contact referring school.
▪ Students are not permitted to use email at REACH. Staff are not normally permitted to use REACH equipment to access personal emails.
▪ Staff do not access personal or work email whilst supervising students.

Mobile phones – Students
▪ Students can bring mobile phones with them to REACH. However, these are locked away securely for the duration of their time at REACH (access is granted during lunch break).

Mobile phones – staff and visitors
▪ Personal mobile phones are not used by our staff on the premises during working hours. They will be stored in a locked cupboard.
▪ In an emergency, personal mobile phones may be used in an area where there are no students present, with permission from the manager.
▪ Our staff and volunteers ensure that the centre managers telephone number is known to family and other people who may need to contact them in an emergency.
▪ Visitors are requested not to use their mobile phones whilst on the premises. We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where no students are present.

Cameras and videos
▪ Our staff and volunteers must not bring their personal cameras or video recording equipment into the Centre.

▪ A consent form with regard to the use of images / recordings is completed by all students /parents / carers at the start of their time with REACH this lays out how images and recordings may or may not be used. Staff are aware of this information.

Social media

▪ Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
▪ Staff should not accept students / parents / carers as friends due to it being a breach of expected professional conduct.
▪ In the event that staff members name the organisation or workplace in any social media they must do so in a way that is not detrimental to the organisation or its service users.
▪ Staff observe confidentiality and refrain from discussing any issues relating to work
▪ Staff should not share information they would not want students / Parents / Carers or Colleagues to view.
▪ Staff should report any concerns or breaches to the Centre Manager
▪ Staff must avoid personal communication, including on social networking sites, with students or their parents / carers. If a member of staff and a student / students family are friendly
prior to the student attending REACH, this information is shared with the centre manager prior to the student attending and a risk assessment and agreement in relation to boundaries is agreed.

Use and/or distribution of inappropriate images

▪ Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately the DSL must be informed immediately and the incident will be dealt with inline with the Child protection policy.
▪ Staff are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).