

**E-Safety - IT & ACCEPTABLE USE POLICY**

**Responsibilities**The senior management team is responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the Academy / College community.

All members of Reynolds Training Academy should agree to an Acceptable Use Policy. This is clearly set out in the E-Safety Policy.

**The Prevent Duty**The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (such as education establishments) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Educational establishments are in an important position to identify risks within a given local context.

Providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for educational establishments to ensure that children and young people are safe from terrorist and extremist material when accessing the internet in such settings. Educational settings should ensure that suitable filtering is in place.   
  
More generally, Reynolds Training Academy has an important role to play in equipping learners to stay safe online, both in the Academy/College and outside. Internet safety is integral to the training Academy’s curriculum and tutorials around online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

* Internet searches for terms related to extremism
* Visits to extremist websites
* Use of social media to read or post extremist material
* Grooming of individuals

The Prevent Duty requires monitoring and filtering systems to be fit for purpose.

**Photographs and Video**   
The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from students is gained if videos or photos of learners are going to be used.   
  
Staff must be fully aware of the consent form responses from learners when considering use of images. These are completed at the time of induction and held in the learner’s learner file.

**Use of E-Mails**Learners should only use e-mail addresses that have been issued by the Academy/College and the e-mail system should only be used for Academy/College related matters.   
  
**Security and Passwords**Passwords should be changed regularly. Passwords must not be shared. Staff must always ‘lock’ the PC if they are going to leave it unattended.

All users should be aware that the ICT system is filtered and monitored by the IT company.

**Reporting**All breaches of the E-safety Policy need to be raised with the appropriate Line Manager/Programme Manager.

Incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Lead – it is their responsibility to decide on appropriate action.

Incidents that are of a concern under the Prevent Duty should be referred to the Designated Safeguarding Lead immediately who should decide on the necessary actions regarding Safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Personal Tutor/Programme Manager.

Allegations involving staff should be reported to the Principal/CEO. If the allegation is one of abuse then it should be handled according to safeguarding legislation and if necessary the local authority’s LADO should be informed.

Evidence of incidents must be preserved and retained.

**Infringements and Sanctions**Whenever a learner infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the senior management team.

Learners are also informed that sanctions can be applied to E-Safety incidents that take place out of the Academy/College if they are related to the Reynolds Training Academy.

RTA E-Safety, IT and Acceptable Use Policy – reviewed 8-8-2023 / 29-2-2024