



BLEND YOUTH PROJECT

INTERNET & ICT SAFETY POLICY

NOVEMBER 2025

Alternative Education Internet & ICT

Acceptable Use Policy

This policy describes the practices and procedures to be followed for the safe and responsible use of Blend Youth Project computer systems, email and for accessing the internet. It includes e-Safety and the rules in place to protect students and Blend Youth Project by describing acceptable / unacceptable internet use.

Why is internet use important?

- The purpose of internet use is to raise educational standards, to promote student achievement and to support the professional work of staff.
- Internet access can be an entitlement for students who show a responsible and mature approach to its use, when needing to research specific information relating to courses they are undertaking.
- Internet use is integral to certain courses and qualifications, as well as being a key skill for independent living and is therefore a vital element of education delivery for those students on long-term placements and/or placements which form the bulk of a student's education provision.

This will enable staff working with children and young people to:

- learn about the potential safeguarding risks to children and young people online.
- learn about the potential risks to all internet users, regardless of age, so that information passed to students is relevant going forward.
- take appropriate steps to develop, update and review child protection policies to keep children and young people safe online.
- provide guidelines for staff and volunteers who use social media as part of their work.

The internet, mobiles phones, social networking and other interactive services have transformed the way in which we live. Children and young people are amongst the early adopters of new technologies and use various interactive services and devices to communicate, interact, create and share content with family and friends. An awareness of these technologies is a vital element of safeguarding and essential as part of a modern education provision.

Online communication mediums are dynamic, constantly evolving with content being generated and easily (and instantly) shared with others. Businesses, advertisers, and other organisations use online services and social media to reach, communicate and engage with young people.

Whilst online resources and technologies are becoming an almost essential element of daily life and can offer tremendous opportunities for young people, as with any environment, there are also risks.

Risks associated with the internet, mobiles and social networking sites and other interactive services include:

- cyberbullying
- grooming
- potential abuse by online predators
- identity theft
- exposure to inappropriate content, including self-harm
- exposure of personal details
- exposure to, or involvement in, racism, sexism and homophobia
- hate speak
- adult pornography.

Some of these risks may be the same as those that young people experience offline. However, they can be more extensive and overwhelming in an online context, because many children and young people fail to realise that the internet is a public place, that content can spread rapidly, and that it is beyond their control once posted publicly. Due to the use of algorithms by media platforms, the quantity of inappropriate or simply negative/unhealthy content a young person is exposed to can also spiral rapidly.

We therefore have an important role to play in educating children and young people on how to stay safe online and encouraging safe and responsible use of social media and internet technologies.

There is also concern that the capabilities of social networking services may increase the potential for sexual exploitation of children and young people. Exploitation can include exposure to harmful content, including adult pornography and illegal child abuse images, as well as direct grooming for the purposes of exploitation.

Online safety information for staff and students

As a provider of education, Blend Youth project (BYP) will make sure that staff are aware of the online risks and the need to protect their own privacy online.

Rules for Employees

- An email address is provided for responsible use in the context of BYP business and should not be used in any other way whatsoever.
- Messages should be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and forwarding of chain letters are not permitted.
- Only official email addresses should be used when contacting schools/referring agencies and professionals involved with young people.

- Take care not to reveal confidential or sensitive information through email, personal publishing, blogs or messaging. Use of BYP ICT equipment and email addresses for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- Only software packages properly authorised and installed by BYP may be used on company equipment, therefore, you must not load any unauthorised software onto BYP computers.
- You must not refer to Blend Youth Project or its services, or represent yourself on behalf of the company on social media, without formal permission from the company to do so.
- Staff should understand the risks in posting and sharing content – even on personal social media profiles - which may damage their reputation.
- Staff should not give out their personal mobile numbers or befriend students online, including on social networking sites.
- Staff should employ privacy settings that make it difficult for students to locate and/or identify them online.

Responsibilities of Staff

Blend Youth Project staff will:

- Discuss and demonstrate safe use of the internet, including regular sessions for all students on e-Safety.
- Closely supervise students who are using computers with internet access.
- Set appropriate levels of internet security on all computers to restrict access to inappropriate materials.

Continuous Professional Development of Staff

- Blend Youth Project will provide staff training on e-Safety as part of all employees' CPD plans.

What is cyberbullying (Bullying online)?

Taken from The Department of Education report 'Preventing and Tackling Bullying' *'The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying which can happen 24/7, with a potentially bigger audience, and more accessories as people forward on content at a click.'*

In many cases, children do not consider particular acts of behaviour to be cyberbullying. For example, saying hurtful things or passing on images are not seen as bullying [by some children], because they happen in cyberspace as opposed to face-to-face. This is often compounded by the impersonal nature of online communications. Although emoticons can be used to clarify intentions, people do not have the benefit of seeing subtle cues and body language that occur with regular human interactions. This can create an intention gap: the victim can interpret what is perceived as a joke by the perpetrator differently. Thus, the definition of cyberbullying must consider and focus on the intensity and harm caused.

The following categories are considered as cyberbullying:

- Sending threatening or discomfoting text messages to a mobile phone
- Making silent, hoax or abusive calls to mobile phones
- Making and sharing embarrassing images or videos via mobile phone or apps.
- Broadcasting unsuitable web cam/video footage that is threatening or manipulative
- Leaving hurtful messages on social networking sites or sending the same message to that person's peer group
- 'Outing' people by publishing or disseminating confidential information online
- Stealing an online identity in order to cause trouble in that person's name
- Deliberately excluding people from online games or groups
- Setting up hate sites or hate groups against an individual
- Sending menacing or upsetting responses in chat rooms, online games, or messenger 'real time' conversations
- Voting for someone in an insulting online poll
- Sending someone 'sexts' that try to pressure them into or expose them to sexual acts

Some of these behaviours or activities are illegal. A person involved could be investigated by the police and prosecuted.

Procedures for preventing cyberbullying

Mobile phones - All UK mobile phone providers have call centres and/or procedures in place to deal with issues around bullying. You can advise that it may be possible to get the student's number changed via their mobile phone provider if they are being bullied. Also, if a certain type of handset is being used then it may be possible to set the phone so that it does not receive phone calls or text messages from a particular number.

Social networking sites - Social networking sites like Facebook have reporting procedures and a safety centre which contains advice for children, young people, parents and professionals. They will remove content that breaches their terms and conditions. Facebook also operates something called 'social reporting'. This encourages people to work with others in their community to report offensive content as well as reporting it 'officially' through Facebook. It is important to remember that the official age for having a Facebook account is 13. However, as it stands, it is quite easy for a young person to set up an account if they are underage by giving a false date of birth.

Video and picture hosting sites - For such hosting sites including YouTube and TikTok, where there are moving images or static pictures posted that are of a bullying nature, you can also report them in the same way you do through social networking sites. Before you report things you may have to create an account if you don't already have one and when you do make a report, it's important to remember that you need to flag things that are deemed inappropriate in the web site's respective policy.

Instant messaging and chat rooms - Instant messenger sites such as Instagram, Facebook and SnapChat are popular methods of communication for young people but can leave them open to being the victim of cyberbullying or sending messages themselves to others that could be seen to be offensive and upsetting. It's important that if bullying has occurred in this context,

that all messages are recorded and archived so that if a report needs to be made or evidence needs to be saved, then there is a clear record. As with other online services, reports can be made about posts/messages that breach the terms of service. It is worth noting that certain sites now remove content once read, so it may be necessary to make notes / take screenshots of any potentially abusive messages seen for later reference.

How will students learn to evaluate internet content?

- If staff or students discover unsuitable sites, the URL (address) and content should be reported in the first instance.
- Blend Staff should ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students should be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Students should be taught to cross-reference, rather than accept the first result delivered by an internet search as factual.

How will the risks be assessed?

- Blend staff should take all reasonable precautions to ensure that students only access appropriate material on BYP computers, including having internet restrictions in place and supervising student use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 – students should be made aware of this as part of their induction.
- Concerns or complaints around a student's internet activity – whether on BYP computer equipment or on a student's personal phone – should be reported to a manager promptly and passed to parents/referring schools & agencies/the police as appropriate, whether this has occurred in education time or not.
- Whilst students are in general allowed to bring in mobile phones for use at break times, where this proves to be problematic, restrictions can be put in place on an individual basis.

General Guidelines for Practice

- Educate students to understand the positive use of ICT, such as to facilitate learning, doing research and to further develop ICT skills.
- Do not let students have access to WiFi passwords at any Blend Sites.
- Do not let students have unsupervised access to ICT equipment where they could easily access social media sites.
- Encourage students to turn their mobile phones off and put them away at the start of each session, all day if possible.
- Be aware that students using mobile phones during break times may have data credit and could be engaging in inappropriate internet use whilst technically under the 'supervision' of Blend staff.

- During break times, structured activities should be available for students to engage in – either individually or together – with the aim of discouraging students from entertaining themselves with phones.