Felixstowe Youth Development Group

Policy Number 20

E-SAFETY POLICY
(Covering all forms of Information Technology)

(Issue 9 – May 2021)

Approved by Trustees _____

Registered Charity Number: 1102380

Registered Address: 2ⁿᵈ Floor, 54 Cobbold Road, Felixstowe IP11 7EL

E-SAFETY POLICY

E-MAIL AND INTERNET

1. Purpose

The purpose of this Policy is to ensure that all staff are aware of the acceptable, safe use of these media. This Policy must be read in conjunction with the Digital Images Policy (No 33).

2. Policy

Level Two expects that staff will not use the e-mail system or internet access to store, display, generate and/or pass on to others material whether in text, pictures or any other form which may be regarded offensive on race, sex, disability, age or any other grounds. LevelTwo understands that it is not always practicable to control the flow of such materials inwards, but this does not take away the responsibility of internal users for any such material they store or pass on. Level Two will not accept that a staff member was not aware that an inappropriate attachment was forwarded, as an excuse for the distribution of offensive material,

3. E-Mail and Internet Use

The e-mail system and Internet access software on Level Two computers is provided for business use purposes only. Though limited personal use is acceptable, staff are not permitted to set up personal accounts on the Level Two server. Level Two has the capacity to (and reserves the right to) access, review, store copy and delete any messages and to disclose them to any person, in each case, as it sees fit for the protection of its business. Level Two reserves the right to monitor and record details of the internet sites accessed and the duration and timing of that access, as necessary for the proper protection of its legitimate business interests.

4. E-Mails as legal documents

As with all other business correspondence, e-mails are disclosable during legal proceedings if they are relevant. Level Two's requirement is that you do not, by e-mail generate, display, distribute or pass on any material any part of which, from timing down to punctuation, you would not be prepared to justify in Court. The misuse of Level Two's e-mail and Internet access systems, deliberate or inadvertent, will be treated as a serious disciplinary matter.

If conducting dealings with outside companies, suppliers etc. by e-mail remember that you could inadvertently create a binding contract with that third party. You should only deal with third parties by e-mail if your job requires it. Use of the e-mail system to copy and/or transmit any documents, software of other information protected by the copyright laws is prohibited.

5. Computer safety, viruses etc

E-mail is one of the most likely points of access of a virus into Level Two's computer systems. Staff must always take care about opening attachments within e-mails.

6. Use of mobile telephones, including Social media and Messenger.

Staff at Level Two are issued with a work mobile phone; these are solely for use on Level Two business. Staff are asked not to use their own mobile phones to safeguard themselves, as well as young people. Any texts or conversations that raise safeguarding concerns should be logged & reported to the Designated Safeguarding Lead (DSL). (Policy No. 3). Level Two staff should not have any work-related young people on any personal social networking site.

6.1 Mobile phones equipped with cameras.

Staff must not use their personal phone to capture digital images of young people. Level Two equipment should be used, in accordance with the Project's Digital Image Policy (No 33).

7. E-safety and Young People

The Level Two Youth Project provides computers in the main body of the hub for use by young people under supervision. Young people using Level Two internet facilities are required to abide by an Internet Safety Agreement, displayed on a poster near the computers, (see Appendix 1 of this Policy), which is informed by the overarching 'Respect' Code of Conduct for Young People, as detailed in Policy No 4.

Internet safety/security software programmes have been installed to prevent access to potentially harmful and unsuitable sites. The software is reviewed and updated regularly to ensure continuity of cover.

8. Level Two Website (www.leveltwo.org)

The website is under the editorial control of the Project Administrator.

Appendix 1

'Safer Surfing'   Internet Safety Agreement
By using Level Two computers in the open area, you agree to:

- Log off when you have finished.

- Keep food and drinks away from the computer desks.

- Log off any social network or chat room sites if you move away from your computer.

- Use 'privacy settings' when messaging, whenever possible.

- Keep your messaging respectful and understand that 'cyber-bullying' is unacceptable.

- Not alter any security settings or move display screens without permission.

- Respect other people and be aware of what you are sending and receiving.

- Not copy any copyrighted material.

- Never intentionally view, share, write, message or download web pages, images or material that is, or may be, considered offensive or disrespectful to others.

- Not open files that are from people/organisations you do not know, e.g. Junk e-mail & messages, as they could contain a computer virus or inappropriate images.

- Think carefully before disclosing any personal details online, such as your real name, date of birth, messenger ID, e-mail address, mobile number or any pictures of your family, friends or yourself.

- Be aware that any picture you send could be changed or shared without your knowledge.

- Be careful who you 'accept' online. Do not add people you do not know to your personal social network sites.

- Never meet up with any strangers, except in the company of an adult you trust.

- It's never too late to tell a Level Two member of staff if you feel unsafe.

If you chose to ignore this agreement, Level Two staff will act to ensure your safety, and the safety of others, in accordance with 'The Level of Respect' Code and/or the Project's Child Protection Policy. For more information on safer surfing visit: WWW.thinkyouknow.co.uk/11-16

ZIP IT
Keep your personal stuff private and think about what you say and do online.

BLOCK IT
Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT
Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.