E-safety Policy.V1.2

Last reviewed:	August 2022
Next review date:	August 2023
Written by:	Bhavini Mistry

Use of Computers, Confidentiality, the Internet and social utility sites

Young people's privacy is respected, their dignity encouraged and information confidentially handled. Staff and young people are kept safe and identities are protected.

Clover Learning Community will take positive steps to protect the confidentiality of information stored on computer and to prevent unauthorised access and inappropriate use.

Due to the sensitive nature of the work we undertake, we need to protect ourselves personally, as well as the company and our young people.

Clover Learning Community will provide children and young people with computers, printers and access to the internet. These facilities will not be abused, the student's welfare is paramount. We will ensure children and young people are safeguarded.

Student laptops have an online filtering system (Senso) which blocks access to social media sites. Search engines used on student laptops prohibit students from searching and viewing inappropriate content. The DSL will be alerted to any inappropriate activity via our Senso portal and take action accordingly.

Staff assign students with laptops and record the laptop numbers they are working on each lesson. See Appendix A for laptop record sheet.

What we do

Computer users will:
- Take appropriate measures to eliminate unauthorised access to the computer at the time of logging on by enabling the security features available with the machine.
- Enable the computer's screen save facility so that the screen is blanked at regular intervals which reflect the amount of passing people.
- Never leave sensitive or confidential material on their screen when the computer is unattended.
- Lock the screen when the computer is unattended.
- Ensure the computer screen is not easily visible to visitors and
- Delete information once details have been printed if not required to be kept in dedicated files on the computer.

Social Networking sites

- All employees must not use a computer to access any social networking sites during contact time with a student or at any time during their working hours.

- All employees who use such sites out of work time should not disclose any information relating to their place of employment. This includes entering the company's name on your profile information. There should be no mention of any matters related to work, i.e., situations that have occurred, names of houses, names of staff members, names of students, etc on any employee's home page. There should be no mention of work related issues whatsoever. To do otherwise will be in breach of confidentially in addition to failure to follow to instruction.

- Students within our education should not be encouraged to access such sites. If a young person visits such a site in your company you should not take part in such activity and must record that the young person has accessed such a site in the young person's daily log. If a

young person has been granted permission to use such a site they need to be supervised during this time.

- All employees should never accept or instigate any contact on any such sites, including emails from the young people within our education, either presently or historically. Any such attempts at making contact with you should be immediately reported to your line manager.

We are encouraging all employees to be very aware that such social utility sites leave individuals vulnerable to the disclosure of personal information and therefore we are reminding everyone that they should use such sites with care and attention relating to who they make contact with.

Clover Learning Community staff must ensure:
- Young people are supervised when using IT Equipment.
- Computer equipment is looked after and any faults are reported straight away.
- Computers and printers are switched off when not in use.
- Young people share the facilities and take into account the needs of others.
- Staff and young people handle the equipment gently.
- Nobody eats or drinks in close proximity to the equipment.
- Young people don't send abusive, threatening or intimidatory e-mails or messages to anyone.
- Young people don't download files etc... without permission.
- Young people don't access illegal pornographic material.
- Young people don't tamper, try to repair, or relocate any equipment.

Use of mobile phones

Staff are allowed to bring their personal phones to work for their own use but will limit such use to non-contact time when pupils are not present. Staff members' personal phones will remain in their bags or cupboards during contact time with pupils.
Staff will not take pictures or recordings of pupils on their personal phones or cameras. If it is necessary when students are taken off site, staff must use the provision's cameras.
We will follow the General Data Protection Regulation and Data Protection Act 2018 when taking and storing photos and recordings for use in the provision.

This Policy will be reviewed annually or sooner if Risk Assessments raise concerns.

This policy is use in conjunction with the Staff Handbook and the Safeguarding Policy.

APPENDIX A – LAPTOP USE RECORD SHEET

Student name	Learning session	Laptop number	Date	Time out / time in