CLOVER LEARNING COMMUNITY

E-safety Policy.V1.5

Last reviewed:	August 2025
Next review date:	August 2026
Written by:	Jadie Wardle

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's have access to the provision's wi-fi network before lessons begin, at break and lunch time.

Student laptops have an online filtering system (Ubiquiti Unifi Dream Pro Gateway) which blocks access to harmful content. Search engines used on student laptops prohibit students from searching and viewing inappropriate content.

The Ubiquiti Gateway blocks harmful content on student laptops and students mobile devices when the provision's wi-fi network is accessed. The system's dashboard shows users activity access time, website access and download information. The DSL will monitor the Ubiquiti on a regular basis and liase with the IT coordinator to ensure all updates are carried out on the Ubiquiti Gateway.

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

Clover Learning Community's staff understand the 4 areas of online risk for young people and children. These are known as the 4 Cs of online safety: Content, Contact, Conduct and Commerce. The terms are defined below:

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism; someone with extreme views may radicalise others online through:

- posts and discussions in web forums
- sharing content on social media and video streaming platforms
- group chat or direct messages in encrypted messaging services

(Staff at Clover Learning Community are all in receipt of regular through on radicalisation through Prevent training and know to follow Prevent guidance https://www.gov.uk/government/publications/prevent-duty-guidance immediately if they suspect a young person is being radicalised.)

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce
Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly.

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 referred to the provision have had their induction and signed their 'Student acceptable use agreement' prior to being issued with a laptop for learning purposes
- 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.

Cyber Bullying

All staff at Clover Learning Community understand that young people and children are capable of abusing their peers online and are at risk of being bullied by other online users. Cyberbullying, along with all other forms of bullying, will not be tolerated here. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Use of mobile phones

Students are allowed to bring mobile phones into provision. Students only have access to the student WIFI during break times as student WIFI does not work during lesson times. Students are not allowed to use mobile phones in lessons and they should be kept in their bags or handed to the learning mentor. Students are not permitted to take photos or videos of staff or students throughout the learning day.

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, the Safeguarding Policy and Anti-bullying Policy.

APPENDIX A – LAPTOP USE RECORD SHEET

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

Appendix B ‘Student Acceptable use Agreement

Student ICT Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context and promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

As with all risks, it is impossible to eliminate them completely and it is therefore essential, through good educational provision, to build resilience to the risks which children and young people may be exposed so that they have the confidence and skills to face and deal with these risks.

This Acceptable Use Agreement is intended to ensure:

- that children and young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that Clover Learning Community’s ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

Clover Learning Community will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement:

I understand that I must use Clover Learning Community’s ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that Clover Learning Community will monitor my use of the provisions ICT systems, email and other digital communications
- I will be responsible and sensible about ICT communications with students, learning mentors and other staff
- I will treat my username and password with care – I will not share it, nor will I try to use any other person’s username and password. I will change my password regularly
- I will be aware of “stranger danger”, when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

Signed: ______________________________________

Print name: ___________________________________

Date: ____