



Policy Review Record

This policy relates to all premises under the governance of the Melton Learning Hub social enterprise. This includes; the Learning Hub and The Venue;

Policy Name: **Melton Learning Hub E-safety Policy**

Date policy written/amended	Amended/written by	Authorised by	Next review due
24 th May 2021	Sarah Cox	Board of Directors 8 th June 2021	June 2022
13.06.22	Sarah Cox	Board of Directors 14 th June 2022	June 2023
01.08.23	Sarah Cox	5 th September 2023	September 2024
02.07.24	Sarah Cox	3 rd July 2024	July 2025

Melton Learning Hub E-safety Policy

1. Introduction

1.1 Melton Learning Hub recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning. This policy is prepared with reference to Keeping Children Safe in Education 2024.

1.2 As part of our commitment to learning and achievement we at Melton Learning Hub want to ensure that the Internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

To enable this to happen we have taken a whole school approach to E-safety as promoted by British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

An important step in improving online safety at our centre is identifying what the potential risks might be.

KCSIE2024 groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract).² These are known as the **4 Cs of online safety**.

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.

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.

- 1.3 Melton Learning Hub and all associated locations as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow disabled pupils increased access to the curriculum and other aspects related to learning.
- 1.4 Melton Learning Hub is committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the risks that exist so that they can take an active part in safeguarding children.
- 1.5 The nominated senior person for the implementation of the Hub's e-Safety policy is Sarah Cox

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), hub governors and volunteers;
- all aspects of the Hub's facilities where they are used by voluntary, statutory or community organisations.

2.2 Melton Learning Hub will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the Internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the Internet and digital technologies;
- education that is aimed at ensuring safe use of Internet and digital technologies;
- a reporting procedure for abuse and misuse.
- A firewall system to protect accessibility on all MLH digital technologies.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Melton Learning Hub recognises that as part of its safeguarding responsibilities there is a need to work in partnership however all information shared with partners will be initialised or encrypted where it refers to confidential information. All learners and families must agree to information being shared with education partners at the commencement of their placement.

3.1.2 Melton Learning Hub will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisations take an approach to their activities that sees the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns. The Melton Learning Hub has a firewall in place which is renewed each year.

4. Policies and Procedures

We at Melton Learning Hub understand that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist within Melton Learning Hub are aimed at providing a balance between exploring the educational potential of new technologies safeguarding pupils.

4.1 Use of Internet facilities, mobile and digital technologies

- 4.1.1 Melton Learning Hub will seek to ensure that Internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.
- 4.1.2 Melton Learning Hub expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:¹ These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the Hub's ICT facilities and digital technologies.

Users shall not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
 - Indecent images of children
 - Promoting discrimination of any kind
 - Promoting racial or religious hatred
 - Promoting illegal acts
 - Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material

4.1.3 The Hub recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. These sites will be supervised by staff and must only be visited for research or educational purposes. Such visits must be authorised by a manager.

4.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Grooming
- Software piracy
- Other criminal activity

4.1.5 In addition, users may not:

¹ For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

- Use the Hubs broadband facilities for running a private business;
- **No child will use the computers without supervision**
- **Computers will be locked away when not in use. The computer rooms at the Hub and the Venue will be locked when not supervised.**
- **Staff computers will be locked when staff are away from the screens**
- **No student will be allowed to use their own mobile phone during lesson time.**
- Enter into any personal transaction that involves The Melton Learning Hub in any way;
- Visit sites that might be defamatory or incur liability on the part of The Melton Learning Hub
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of The Melton Learning Hub;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
 - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via The Melton Learning Hub
- Undertake activities with any of the following characteristics:
 - wasting staff effort or networked resources
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using the MLH network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - other misuse of the embc network, such as introduction of viruses.
- Use any mobile or digital technologies 3G or mobile Internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

- 4.1.6 Where the Melton Learning hub become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

- 4.2.1 There will be occasions when either a pupil or an adult within the Hub receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the Hub is that the pupil or adult should be report the incident **immediately**.
- 4.2.2 The Hub also recognises that there will be occasions where pupils will be the victims of inappropriate behavior and potential grooming, that could lead to possible or actual significant harm, in such circumstances LSCB² Procedures should be followed. The response of the Hub will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the Hub will refer details of an incident to the lead agencies involved in safeguarding children, namely Children's Social Care and the Police.

The Hub, as part of its safeguarding duty and responsibilities will, in accordance with LSCB Procedures³ assist and provide information and advice in support of child protection enquiries and criminal investigations.

5. Education and Training

- 5.1 Melton Learning Hub recognises that the Internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.
- 5.2 As part of achieving this, we want to create within Melton Learning Hub an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.
- 5.3 To this end, Melton Learning Hub will:-
- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the Hub curriculum.

- Educate Hub staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the Hub.

6. Standards and Inspection

Melton Learning Hub recognises the need to have regular inspections of policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring

6.1.1 Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and electronic mail a pupil or member of staff may have. Melton Learning Hub recognises that in order to develop an effective whole Hub E-safety approach there is a need to monitor the students when they are accessing the internet on centre computers.

6.1.2 Mobile technologies will only be allowed to be used by students at breaktimes. If a student gets their phone out it will be put on charge or in a tray in the corner of their classroom to prevent use and disruption to learning. **No students will be given the wi-fi codes for an Melton Learning Hub site.**

6.1.2 Another aspect of monitoring, which our Hub will employ, is the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that Hub staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.1.4 Emergencies- In an emergency where a staff member is called away all computers will be turned off at the main switch or locked by the member of staff. However if the staff member does not have time to do this then they should escort students out of the room and lock it, until their return.

6.2 Sanctions

6.2.1 Melton Learning Hub has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the centre to manage such situations in, and with, confidence.

6.2.2 Where there is inappropriate or illegal use of the Internet and digital technologies, the following sanctions will be applied:

- *Child / Young Person*
 - The child/young person will be disciplined according to the behaviour policy of the school, which could ultimately include the use of Internet and email being withdrawn. A request will also be considered for the young person to not bring mobile technologies to centre.
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- *Adult (Staff and Volunteers)*
 - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
 - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

7. Working in Partnership with Parents and Carers

7.1 *Melton Learning Hub* is committed to working in partnership with parents and carers and understand the key role they play in the Internet safety of their children, through promoting Internet safety at home and elsewhere.

7.2 We at Melton Learning Hub also appreciate that there may be some parents who are concerned about the use of the Internet, email and other digital technologies in Hub. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

8. Appendices of the E-safety Policy

8.1 Social media top tips for parents.

8.2 The Staff Handbook provides more guidance on rules and expectations of Staff

8.3 The Safeguarding policy refers to all aspects staff need to be aware of that might present a danger to children including online activity.

Appendix 1- Social Media Awareness Top Tips

- Talk to your child about online grooming
- Talk to them about their online friends
- Let your child know that you are always there for support and you understand how easy it is for things to get out of control online
- Learn how to report any inappropriate contact made to your child online
- Security settings need to be set to “Friends only”, that includes comments, posts and photos
- These “Friends” need to be people they know and trust in the real world
- Content Only post content and photos they wouldn’t mind showing you!
- Try your very best to be “Friends” with your child on Facebook • Learn how to report an issue directly to Facebook
- Help set up their profile
- Add your email as the main contact (if possible)
- Set the privacy settings to “friends” only and ensure they are children you know
- Show them a CEOP safety resource which outlines the risks: www.youtube.co.uk/ceop/jigsaw
- ‘Like’ the Click CEOP page
- Check in and keep updated
- Leave all gaming devices in a family
- Open up communication talk to your child about the sites they are using and why they like them
- Explain that people lie online and they are not always who they say they are
- Ask them to never give out personal information
- Set parental controls
- Explain that people can be mean online and don’t always have their best interests at heart
- Set time limits on how long they can game for. Allow time for nontechnology based activities and allow an hour ‘screen free’ time before bed
- Ask your child to never accept people they don’t know and trust in the real world
- Inform them that giving out personal information can be dangerous. They need to treat personal information such as the school they go to or their location like their tooth brush and not share it with anyone!



Appendix 2- Mobile Phone – Guidance

- Mobile phones may be used on centre grounds before lessons, during lunch, and after lessons have finished.
- Mobile phone use is prohibited in classrooms, restrooms, and offices, unless otherwise stated by a tutor.
- During the instructional day, mobile phones must remain out of sight and in silent mode.
- Unless explicitly allowed by a staff member, headphones and other listening devices may only be used before and after centre hours.
- Mobile phones must be placed in bags, or another location away from students and their desks during tests and assessments.
- If students need to place an emergency phone call during the day, they should request to go to the main office to use an office phone.
- Students may be subject to disciplinary action if their use of their mobile phone disrupts the school's educational environment:
 - 1/ Step one will be a request to parents to advise their child of appropriate use of their phone at centre.
 - 2/ Step 2 is a letter home warning that a continued breach of the rules will result in a phone ban.
 - 3/ Step 3 is a letter home informing the child's parents/ guardian that their child will not be allowed to bring their phone to centre. Any breach of the ban will result in the child being sent home.
- The centre and its staff are not responsible for any damage to or theft of a student's mobile phone. Students must properly secure and take care of their own phones.
- Students and their parents must read the mobile phone policy and return a signed copy to the office at the beginning of the school year. Signing the policy acknowledges acceptance.

Child's name.....

Signed and acknowledged by parents/ guardians
name.....

Signature.....

Dated.....