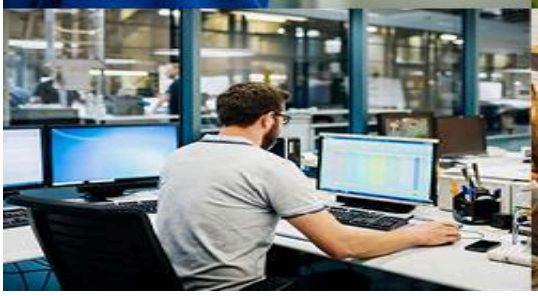
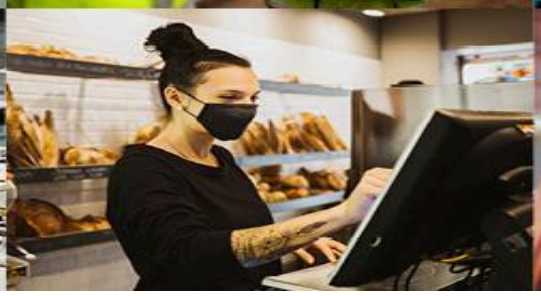
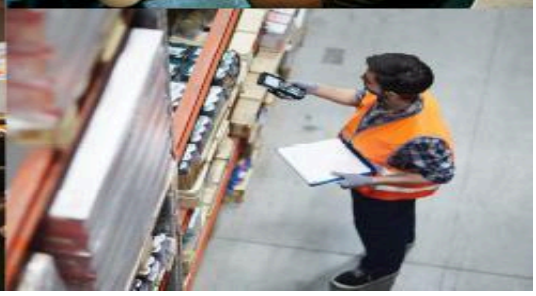
EARLY LIFE

ENTERPRISE | ENGAGE| INSPIRE

E-Safety Policy

Last reviewed on:	1st september 2025
Next review due by:	1st September 2026
Signed by	
Position	Director / Head of Centre



We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our provision aims to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers
- Protect and educate the students and staff in their safe and responsible use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Set clear guidelines for the use of mobile phones in the provision
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate
- Educate pupils about online safety as part of our curriculum. For example:
- The safe use of social media, the internet and technology
- Keeping personal information private
- How to recognise unacceptable behaviour online
- How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they're a witness rather than a victim
- Train staff on safe internet use and online safeguarding issues including cyber-bullying, the risks of online radicalisation, and the expectations, roles and responsibilities around filtering and monitoring. All staff members will receive refresher training as required and at least once each academic year
- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
- Staff are allowed to bring their personal phones to the provision for their own use, but will limit such use to non-contact time when pupils are not present
- Staff will not take pictures or recordings of pupils on their personal phones or cameras
- Make all pupils, parents/carers, staff and volunteers aware that they are expected to sign an agreement regarding the acceptable use of the internet in provision, use of the provision's ICT systems and use of their mobile and smart technology
- Explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones
- Carry out an annual review of our approach to online safety.
- Provide regular safeguarding and child protection updates including online safety to all staff, at least annually, in order to continue to provide them with the relevant skills and knowledge to safeguard effectively
- Review the child protection and safeguarding policy, including online safety, annually and ensure the procedures and implementation are updated and reviewed regularly

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism, disinformation, misinformation and conspiracy theories

Disinformation is the deliberate creation and spread of false or misleading content, such as fake news. **Misinformation** is the unintentional spread of this false or misleading content (Cabinet Office, Department for Science, Innovation and Technology, 2023).

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1.Introduction

The e-Safety Policy is part of, and relates to other policies including those for;-

• Anti-bullying Policy

• Attendance, Behaviour and Behaviour Management Policy

• Safeguarding Policy

Learners are encouraged to access internet resources as part of their education at Early Life Enterprise Learning.

We recognise that children and young people may expose themselves to danger, whether knowingly or unknowingly, when using the internet. We therefore recognise our responsibility to educate our students about appropriate behaviour when using the internet and critical thinking skills to enable them to remain both safe and legal when using the internet.

As Designated Safeguarding Lead, Annecia Warburton, has overall responsibility for internet safety and the DSD, Ian Lawrence, acts as our E-Safety Coordinator. Teachers/staff at Early Life Enterprise are responsible for overseeing the use of internet and email by students on premises.

The internet is used at Early Life Enterprise's to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance Early Life Enterprise's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education, and business. We want to equip our students with all the necessary ICT skills that they will need to enable them to progress confidently into a professional working environment and/or further study.

2. Roles and responsibilities

2.1 The managing partner

The managing partner is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the provision.

2.2 The designated safeguarding lead/Deputy

Details of the provision's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSD takes lead responsibility for online safety in provision, in particular:

- Supporting the managing partner in ensuring that staff understand this policy and that it is being implemented consistently throughout the provision
- Working with the managing partner and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the provision child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the provision behaviour policy

- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in provision to the managing partner

This list is not intended to be exhaustive.

2.3 All staff and volunteers

All staff, including contractors and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the provision's ICT systems and the internet, and ensuring that pupils follow the provision's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the provision behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

2.4 Parents

Parents are expected to:

- Notify a member of staff or the managing partner of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the provision's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

2.5 Visitors and members of the community

Visitors and members of the community who use the provision's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

3. Enhancing Learning

Increased computer numbers and improved internet access may be provided but its impact on students learning outcomes should also be considered. Developing effective practice in using the internet for teaching and learning is essential. Students need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught; students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work. Methods to detect plagiarism may need to be developed.

EARLY LIFE ENTERPRISE will ensure that the copying and subsequent use of internet-derived materials by staff and students complies with copyright law.

Early Life Enterprise's internet access is designed to enhance and extend education. Staff should guide students to online activities that will support the learning outcomes planned for the students' age and ability.

Students will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.

Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students. Filters are in place.

Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation.

4. IT Access

Students may be given to access to a computer and the internet via Early Life Enterprise laptops. Students will never have access to the internet except under direct supervision by staff. Students will never be left unattended with a laptop.

Staff will make sure that student's login to these laptops via a guest login, which is void of any sensitive or protected information. Any work that students complete will be saved to a secure external drive or emailed. Staff should refer to the 'Staff Code of Conduct' for more information on appropriate use of devices.

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the provision behaviour policy.)

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The provision will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the provision will follow the processes set out in the provision behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the provision will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

5.3 Examining electronic devices

The managing partner, DSL, and any member of staff authorised to do so, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the provision rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the managing partner or DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the provision or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and managing partner decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the provision complaints procedure.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded

• 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre - NCSC.GOV.UK.

6. Acceptable use of the internet in provision

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the provision's ICT systems and the internet. Visitors will be expected to read and agree to the provision's terms on acceptable use if relevant.

Use of the provision's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers and visitors (where relevant) to ensure they comply with the above.

6.2 Use of Generative AI

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Early Life Enterprise CIC recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Early Life Enterprise CIC will treat any use of AI to access harmful content or bully pupils in line with this policy and our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out risk assessments for any new AI tool being used by the school.

Staff and pupils must follow the same Acceptable Use Policy principles extended to AI use:

- No confidential or personal data should be shared with third-party AI tools
- AI usage does **not** replace human accountability—**all output must be reviewed** before use
- AI-generated content should be disclosed where it contributes ≥ 25% of final output.
- Use of AI must be transparent—any AI contribution must be acknowledged in student work or communications.
- Only AP approved AI tools should be used and staff should operate them through AP-provided accounts.
- Parents and carers will be informed about AI usage in provision and provided support through constant communication channels to ensure families understand both the benefits and risks of AI in their children's education and can raise concerns as needed.

Filtering and monitoring of generative AI will be in line with the DfE guidance GenerativeAI: product safety expectations
https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations

Generative AI tools used must be:

- Reviewed for safety and compliance with the DfE's **"Generative AI: product safety expectations"**
- Subject to the same filtering/monitoring protocols as other online tools.
- Ensure aligned with **cyber-security standards**, including safe device use and protection from malicious AI-generated content
- The DSL will oversee AI's impact on student safety and risk assessments will be completed to help monitor and mitigate potential security, legal and ethical risks.
- Any AI related incidents such as data breaches or inappropriate outputs, will be reported promptly to the DSL through standard safeguarding channels.
- Disciplinary action will be taken for misuse of AI.

Staff and directors receive training on AI's advantages, risks, and ethical considerations. This ensures that both educators and administrators are equipped to use AI effectively and responsibly. Learners are also educated on the ethical use of AI, helping them develop critical thinking skills and awareness of AI-related risks.

7. Pupils using mobile devices in provision

Pupils may bring mobile devices into provision, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after provision, or any other activities organised by the provision

Any use of mobile devices in provision by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the provision behaviour policy, which may result in the confiscation of their device.

8. Staff using work devices outside provision

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the provision's terms of acceptable use.

Work devices must be used solely for work activities.

9. How the provision will respond to issues of misuse

Where a pupil misuses the provision's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the provision's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The provision will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

11. Handling e-Safety Complaints

Complaints of student internet misuse will be dealt with by the Principal at Early Life Enterprise Any complaint about staff misuse must be referred to the Managing Partner Complaints regarding safeguarding must be dealt with in accordance with Early Life Enterprise's Safeguarding Policy.

Students and parents will be informed of the Complaints Policy, which is available on Early Life Enterprise's website.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for provisions on:

- Teaching online safety in provisions
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and provision staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

EARLY LIFE

ENTERPRISE | ENGAGE | INSPIRE

Email: hello@earlylifeenterprise.co.uk
Web: www.earlylifeenterprise.co.uk