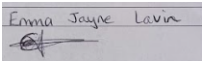
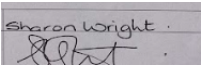




E-SAFETY / ACCEPTABLE USE POLICY

UPDATE MINUTES				
VERSION	DATE	CHANGES	UPDATED BY WHOM	CHECKED BY
VERSION 1	SEPT 24	DEVELOPED AND RE ORDERED LAYOUT	EMMA JAYNE LAVIN	SHARON WRIGHT
VERSION 2	10 FEB 2025	UPDATED / DEVELOPMENT CHECKS	EMMA JAYNE LAVIN	SHARON WRIGHT

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

SUMMARY OF DOCUMENT

The internet is a powerful tool but contains risks such as inappropriate content, cyberbullying, and data privacy issues.

Young people must develop critical thinking skills to assess online content and protect personal information.

The E-Safety policy applies to all internet technologies, including mobile phones, gaming consoles, and wireless devices.

The goal is to educate students on responsible digital behavior at school and home.

E-Safety focuses on safeguarding rather than restricting, promoting informed and responsible use of technology.

Schools have a duty of care to ensure students use online platforms safely.

Online risks include exposure to harmful content, grooming, identity theft, and excessive screen time.

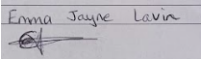
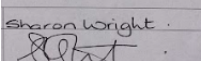
Everyday Lessons incorporates e-safety education into all lessons, teaching research skills, responsible online behavior, and privacy awareness.

Students learn about risks related to sharing personal information, online harassment, cyberbullying, and copyright laws.

The school encourages students to report online concerns to a trusted adult and provides access to external support services like Childline.

The policy aligns with **Keeping Children Safe in Education (KCSIE) 2024**, ensuring compliance with safeguarding measures.

INTRODUCTION

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

The internet is a widely accessible and mostly unregulated communication tool. Websites, emails, blogs, and social media allow people to share information globally at little cost, making it a powerful resource. However, some online content is inappropriate for children, including material related to violence, adult themes, extremism, and other harmful topics. It is essential for young people to develop critical thinking skills to evaluate online content and recognise the dangers of sharing personal information.

Our E-Safety policy covers internet technologies and electronic communications, including mobile phones, gaming consoles, and wireless technology. It aims to educate children and young people on the benefits, risks, and responsibilities of using digital tools. This information aims to support learners beyond the classroom and encourage our learners to use these tools safely when at home.

E-Safety is about safeguarding children in the digital world, promoting positive engagement with technology, and educating them about both risks and advantages. Rather than focusing on restrictions, it encourages informed and responsible online behavior, both in and out of school.

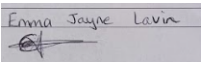
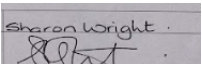
Schools have a duty of care to ensure pupils use online platforms safely.

Incidents involving inappropriate online behavior will be addressed under these policies, with parents/carers informed when necessary.

The online world offers many opportunities for learning and communication, but it also comes with risks. Young people can be exposed to inappropriate content, such as online pornography, violent video games with offensive language, substance abuse, and harmful lifestyle sites that promote self-harm or eating disorders. Hate sites and misinformation are also concerns, making it essential for students to critically evaluate online content for accuracy and authenticity.

Online interactions can also pose risks, including grooming, cyberbullying, and identity theft. Sharing personal details can lead to privacy issues, impacting a child's digital footprint and online reputation. Excessive time spent online can affect mental and physical well-being, and sharing intimate images, known as sexting or SGII (self-generated indecent images), carries serious consequences. Additionally, young people must understand the importance of respecting copyright laws when accessing music, films, and other digital content.

Everyday Lessons incorporates e-safety into its curriculum through a structured and age-appropriate programme within all lessons. Students learn how to verify information, refine search results, and understand how search engines influence what they see. They are taught

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

responsible online behavior, including the importance of politeness, keeping personal details private, and recognising that online 'friends' may not be who they claim to be.

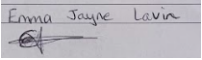
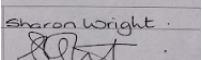
Pupils also gain an awareness of the risks of sharing personal details, photos, and videos, including the importance of obtaining consent before posting images of others. They are educated on the dangers of downloading files without permission and strategies for handling inappropriate content. Understanding the impact of cyberbullying, trolling, and sexting is a crucial part of this programme, ensuring that students know how to seek help if they encounter online abuse.

Everyday Lessons emphasizes the importance of reporting online concerns. Students are encouraged to speak to a parent, carer, teacher, or trusted staff member if they feel unsafe online. They are also made aware of external support services such as Childline. By fostering a responsible and informed approach to online safety, we aim to empower young people to navigate the digital world securely and confidently.

KEY PRINCIPLES

At Everyday Lessons, we are committed to promoting the safe and responsible use of ICT-based technologies. All members of our school community are expected to follow these key principles:

- **Education** - Everyday lessons puts online safety at the forefront of everything we do.
- **Safeguard and Protect** – Ensure the safety and well-being of all children, young people, and staff when using digital technologies.
- **Support Safe Practice** – Enable staff to use the internet and communication tools responsibly while maintaining high professional standards.
- **Establish Clear Expectations** – Set guidelines for appropriate online behavior, covering educational, personal, and recreational use of the internet.
- **Address Online Abuse** – Implement clear procedures for dealing with issues such as cyberbullying, aligning with safeguarding and anti-bullying policies.
- **Enforce Accountability** – Ensure all community members understand that unsafe or illegal online behavior will not be tolerated, and disciplinary or legal action may be taken when necessary.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

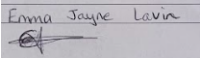
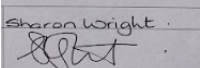
- **Reduce Risks for Staff** – Minimise the chance of false or harmful accusations against adults working with students by promoting transparent and professional online interactions.

STAYING SAFE ONLINE

Social media can have a significant impact on the mental health of children and young people, often leading to anxiety, low self-esteem, and exposure to harmful or inappropriate content. To promote a safer online experience, learners will be encouraged to use privacy controls, activate safety features, and adhere to age restrictions. Staff members must also exercise caution when using social media by regularly reviewing their security settings to protect personal information. They should avoid discussing personal matters related to students, parents, carers, or colleagues and must ensure that any opinions shared online are not mistakenly attributed to the school.

To stay safe online, children and young people should:

- **Protect Personal Information** – Avoid sharing full names, addresses, school details, passwords, or other sensitive data.
- **Think Before You Share** – Be cautious when posting photos, videos, or personal updates, as content shared online can be permanent.
- **Use Privacy Settings** – Adjust social media and app settings to limit access to personal information.
- **Be Aware of Online Strangers** – Never accept friend requests or engage in conversations with unknown individuals.
- **Recognise and Report Abuse** – If someone makes you uncomfortable online, report them to a trusted adult or use the platform's reporting tools.
- **Avoid Harmful Content** – Stay away from websites or social media pages that promote violence, hate, self-harm, or illegal activities.
- **Be Kind and Respectful** – Treat others online as you would in person and never participate in cyberbullying.
- **Check Information Sources** – Not everything online is true. Verify facts from reliable sources before believing or sharing them. This links back to the education in our key principles as we ensure we educate on misinformation and disinformation to ensure learners are critically thinking and fact checking.
- **Use Secure and Trusted Websites** – Look for "https://" in web addresses and avoid suspicious links or downloads.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

- **Take Breaks from Screens** – Limit screen time to maintain a healthy balance between online and offline activities.

At Everyday Lessons, we expect all members of the school community to use ICT systems responsibly and in accordance with our policies. This includes learners, staff, and parents/carers, ensuring a safe and secure digital environment. Our approach aligns with **Keeping Children Safe in Education (KCSIE) 2024**, which emphasises safeguarding learners online, promoting responsible technology use, and ensuring clear procedures for reporting concerns.

Safe spaces online for Teaching and learning - as outlined by ETF (Education and training foundation)

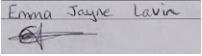
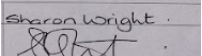
Establishing a safe space for online teaching and learning is essential for fostering an environment where all participants feel secure, respected, and able to engage without fear of harm or discrimination. A safe space is not just about the technology used but also about the behaviours adopted by both educators and learners.

To achieve this, the following principles should be upheld:

- **Do No Harm:** Educators and learners must be aware of behaviours that can cause harm, such as sharing inappropriate content, excessive communication, or engaging in online harassment.
- **Inclusivity:** A Safe Space is one where all individuals feel included and empowered to contribute without fear of discrimination or exclusion.
- **Adaptability & Resourcefulness:** Online learning requires flexibility to address technical challenges, support emotional well-being, and maintain a positive learning atmosphere.

To enable this we must;

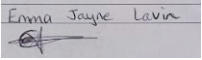
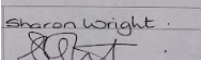
1. **Define Clear Expectations**
 - Establish a working agreement outlining acceptable behaviours, digital etiquette, and consequences for misconduct.
 - Reinforce the importance of respectful communication and engagement.
2. **Encourage Positive Online Behaviours**
 - Model professional and respectful interactions.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

- Address inappropriate behaviour using structured models such as the SAID framework (Standard, Action, Impact, Do/Develop).
 - Promote **digital resilience** by equipping learners with the skills to navigate challenges online.
3. **Recognise and Respond to Risks**
- Train educators to identify signs of **distress, cyberbullying, and online abuse**.
 - Implement clear **reporting pathways** for learners to flag concerns.
 - Ensure compliance with safeguarding procedures, such as the **RESPONSE model**:
 - **Recognise** concerns.
 - **Educate** on risks.
 - **Safeguard** all individuals.
 - **Prevent** potential harm.
 - **Own** responsibilities.
 - **Not alone**—offer support networks.
 - **Signpost** to appropriate services.
 - **Ensure** a culture of trust.
4. **Managing Online Behaviour**
- Understand that online behaviour differs from face-to-face interactions and may require additional clarity in communication.
 - Recognise patterns of behaviour to identify when a learner may be struggling.
 - Use positive behavioural reinforcement, such as encouraging, supporting, and active listening.
5. **Enhancing Digital Safety Measures**
- Use **privacy settings** and security controls to prevent unauthorised access to learning platforms.
 - Ensure all staff and learners understand the **importance of data protection** and responsible sharing of information.
 - Regularly review and update **digital safeguarding policies** to align with emerging risks and best practices.

Embedding these principles into everyday online teaching practices, educators can foster a learning environment that prioritises safety, engagement, and inclusivity. Creating a safe and positive digital environment for everyone at Everyday Lessons.

EXPECTATIONS - LEARNERS /STAFF/PARENTS

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

Staff must:

Staff members at Everyday Lessons have a responsibility to ensure a safe digital environment for all learners. They must familiarize themselves with and adhere to the school's e-safety policy when using ICT systems, including mobile devices. By demonstrating responsible digital behavior, staff serve as role models, reinforcing the importance of safe and ethical technology use. Additionally, they play a key role in safeguarding by recognizing and addressing online risks in accordance with **Keeping Children Safe in Education (KCSIE) 2024**, ensuring that any concerns are reported and managed appropriately to protect learners.

- Adhere to school policies on ICT and mobile device use.
- Lead by example, promoting responsible and safe online behavior.
- Stay vigilant and report any online risks in line with safeguarding guidelines.

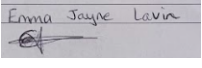
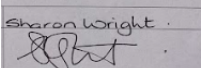
Learners must:

Learners at Everyday Lessons are expected to use school ICT systems responsibly, adhering to policies regarding mobile phones, digital devices, and image usage. They must be aware of the potential risks of accessing inappropriate content and understand the consequences of misuse. Reporting any incidents of abuse, misuse, or exposure to harmful material is essential, and learners should know how to seek help when needed. Their online behavior, even outside of school, must align with school policies if it impacts the school community. Additionally, they should develop strong research skills, respect copyright laws, and avoid plagiarism to maintain academic integrity.

- Use ICT systems responsibly and follow school policies on devices and images.
- Be aware of online risks and the consequences of misuse.
- Report abuse, misuse, or inappropriate content and know how to get help.
- Ensure online behavior, even outside school, aligns with school policies.
- Develop research skills, respect copyright laws, and avoid plagiarism.

Parents/Carers must:

Parents and carers play a crucial role in ensuring their child's online safety. Upon entry to the school, they are required to provide consent for their child's use of the internet and digital technologies by signing the e-safety agreement. It is important for parents to be aware of the

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

potential risks their child may face online and to collaborate with the school in promoting responsible digital habits at home. Understanding the school's policies, including what is considered appropriate use and the consequences of misuse, allows parents to support their child in making safe and informed choices when navigating the online world.

- Give permission for their child to use school internet and digital tools.
- Stay informed about online risks and reinforce safe internet use at home.
- Familiarise themselves with school ICT policies and help children follow them.

CONSENT

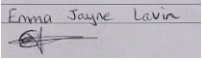
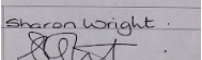
At Everyday Lessons, we obtain parental or carer consent for the use of digital photographs and videos featuring their child as part of the enrolment process. This ensures that all multimedia content used within the school environment is handled appropriately and with full awareness of those involved.

To protect students online, the school actively restricts access to social networking platforms and newsgroups unless their use has been specifically approved for educational purposes. Learners are strongly encouraged to exercise caution when sharing personal images online and are educated on the importance of privacy settings to prevent exposing sensitive information to the public.

Students are also taught that sharing images or videos of others without consent is unacceptable. They receive guidance on the risks associated with posting pictures that may include identifying details, such as file names, locations, or personal data. Additionally, they learn the importance of safeguarding their personal information, maintaining data security, and understanding how to seek help if they experience online harassment or bullying.

REPORTING CONCERNS

Everyday Lessons takes e-safety seriously and enforces its policies with clear and appropriate consequences for any violations. Online activity is closely monitored, with all incidents recorded to enhance policies and ensure learner safety. The entire school community, including learners, staff, and parents, is encouraged to report any e-safety concerns, which are promptly addressed by designated safeguarding leads (DSLs) through established escalation procedures.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

DSL - Emma Jayne Lavin - 07807078976 - Emma@everydaylessons.co.uk

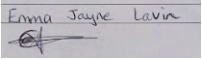
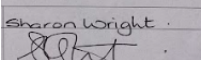
In cases of serious online threats or incidents, external agencies such as The Child Exploitation and Online Protection Centre (CEOP), local authorities, or the police may be involved. Parents and carers are kept informed about any e-safety issues concerning their child, fostering transparency and a collaborative approach to safeguarding. If staff or learners receive online communication that is particularly alarming or illegal, the school will contact the police to take necessary action.

- Strict enforcement of e-safety policies with appropriate consequences.
- Continuous monitoring of online activity to enhance learner protection.
- A clear reporting system for e-safety concerns, managed by safeguarding leads.- This is the same reporting process laid out in the safeguarding policy.
- External agencies consulted for serious online safety threats.
- Parents kept informed about incidents involving their child.
- Police intervention if any online communication poses a significant threat.

By embedding these expectations and procedures, Everyday Lessons creates a safe digital learning environment, ensuring compliance with safeguarding and child safety policy protecting all members of the school community from online harm.

SECURITY AND PRIVACY

Everyday Lessons places great importance on maintaining the security and privacy of all users' digital accounts. Staff and learners must keep their passwords confidential, never sharing them or leaving them in places where others may access them. Each staff member is assigned a unique username and password for accessing school systems and is responsible for ensuring their credentials remain secure. The school provides staff with professional email accounts, reinforcing that personal correspondence should be conducted via separate personal accounts. Given the risks of spam, phishing, and malicious attachments, login details must never be shared. When staff communicate with parents via email, they must use professional language and, in potentially sensitive situations, copy in their line manager or department head. Emails sent externally should be carefully written, adhering to the school's formal communication guidelines, as they represent the institution in the same way as official letters.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

Learners are introduced to email use as part of their digital literacy education, learning how to engage with it safely both within and beyond the school environment. They are taught that emails are a form of published communication and should be clear, concise, and appropriate. Personal details, such as home addresses and phone numbers, must never be shared via email. Learners are encouraged to think critically before opening attachments and only do so if they trust the source. They are also taught to immediately inform a teacher or responsible adult if they receive an email that makes them uncomfortable or contains offensive or bullying content. Additionally, they are instructed not to engage with or respond to harmful messages and to retain any malicious emails as evidence rather than deleting them. Meeting individuals encountered through email is strictly prohibited unless discussed with a trusted adult and accompanied by a responsible adult.

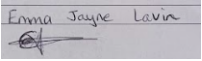
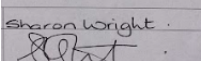
To reinforce these principles, learners sign an Acceptable Use Agreement confirming their understanding of e-safety rules, including appropriate email use. They are made aware of the consequences of misuse, ensuring they understand the importance of maintaining a secure and respectful digital presence.

At Everyday Lessons, the responsible use of digital technology and mobile devices is essential to maintaining a safe and professional learning environment. Social media use within the school is strictly prohibited and blocked where possible. Staff members using school-approved blogs or online accounts must ensure they are password-protected and that their communication remains professional at all times. Discussions about students, parents, or other staff members on social media platforms are not permitted, and personal opinions shared online must not be attributed to the school. To protect personal data, all staff should regularly review the privacy settings on their social media accounts to minimize risks of information exposure.

Mobile phones and personal devices brought onto school premises are the responsibility of the owner. The school accepts no liability for loss, theft, or damage to any such devices. **For students, mobile phones must be switched off (not just placed on silent) and kept out of sight throughout the school day, from arrival until departure.** Staff members should also refrain from using their mobile phones during lesson times, and visitors are required to keep their devices on silent while on-site.

The school enforces strict guidelines on the recording, taking, and sharing of images, videos, or audio using mobile devices. Such actions are only permitted with explicit approval from senior leadership and must be monitored and recorded. Any **unauthorized use of mobile devices for recording or sharing content is strictly prohibited.**

Mobile Phone and Device Rules:

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

- **No personal device use during lessons** unless part of a structured, staff-approved learning activity.
- **Students must keep phones switched off and out of sight** throughout the school day.
- **Visitors must keep phones on silent** while on school premises.
- **No recording, photographing, or sharing of content** unless formally approved.
- **Bluetooth and file-sharing features must be disabled** to prevent unauthorised data transfer.
- Social media use is not permitted in learning centers and is restricted wherever possible.

The school reserves the right to inspect the contents of mobile devices if there is reasonable suspicion that they contain inappropriate material, such as content promoting violence, bullying, or explicit material.

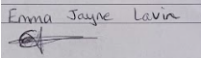
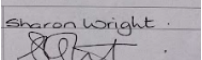
Staff devices may also be subject to routine checks if an allegation has been made.

PERSONAL USE

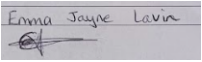
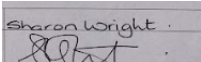
The school has clear guidelines on the use of personal mobile devices to maintain a safe and professional learning environment. Both staff and students must adhere to these policies to ensure responsible and appropriate use of technology.

Students are expected to follow the school's mobile device policy at all times. Failure to do so will result in confiscation, with devices securely stored in the school office. In most cases, a parent or carer will be required to collect the device. Mobile phones and electronic devices are strictly banned in exam settings, and any student found with one during an examination will be reported to the relevant exam board, which may lead to disqualification. If students need to contact a parent or carer during school hours, they may do so via a school phone, and parents are encouraged to communicate through the school office rather than calling or messaging their child directly.

Staff members must also use personal devices responsibly and should not contact students, parents, or carers using their own phones. Instead, all professional communication must take place through designated school phones. During working hours, staff devices should be kept on silent or switched off, and Bluetooth should be disabled to enhance privacy and security. Personal devices must not be used during lessons unless explicitly approved by senior leadership under exceptional circumstances.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026

Both staff and students are encouraged to protect their personal information by only sharing contact details with trusted individuals. The school provides guidance on safe and responsible mobile phone use, helping everyone understand the risks and consequences of misuse. In cases where staff are required to use a phone for school-related duties, such as during off-site activities or emergencies, a school-issued device will be provided. Non-compliance with these policies may result in disciplinary action for staff or further sanctions for students.

Uncontrolled when printed			
Author	Authorised by	Version Number	Issue Date
Emma Jayne Lavin Sharon Wright	Emma Jayne Lavin	2	February 2025
Role	SIGNED	SIGNED	Review Date
Proprietor / QA			February 2026