



Esland North Limited - Exec

ED00400 - Online Safety Policy



Introduction

Esland Online School is committed to providing a safe, secure and supportive digital learning environment for all pupils, staff, volunteers, governors and families.

As a specialist online school, we recognise that technology is integral to teaching, learning, communication and safeguarding. We are committed to promoting a culture of online safety that enables pupils to benefit from technology while being protected from harm.

Online safety is a safeguarding issue and is embedded throughout the school's curriculum, policies, procedures, safeguarding practice and culture.

This policy should be read in conjunction with:

- Safeguarding and Child Protection Policy
- Promoting Positive Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- ICT Acceptable Use Policy
- Relationships and Health Education Policy

Legislative and Guidance Framework

This policy has been developed with regard to:

- Keeping Children Safe in Education (2026)
- Working Together to Safeguard Children (2026)
- Teaching Online Safety in Schools
- Relationships Education, Relationships and Sex Education and Health Education
- Searching, Screening and Confiscation
- Sharing Nudes and Semi-Nudes: Advice for Education Settings
- Prevent Duty Guidance
- UK Council for Internet Safety (UKCIS) Framework
- Data Protection Act 2018
- UK GDPR
- Equality Act 2010
- Education Act 1996
- Education and Inspections Act 2006
- Online Safety Act 2023

Definitions

For the purpose of this policy:

Cyberbullying

The use of technology to deliberately and repeatedly harm, intimidate or harass another person.

Grooming

When someone builds an emotional connection with a child to gain trust for exploitation, abuse or trafficking.

Sextortion

The use of threats, coercion or blackmail involving sexual images, videos or information.

Deepfakes

Images, audio or videos created or manipulated using artificial intelligence to appear genuine.

Misinformation

False information shared without intent to deceive.

Disinformation

False information deliberately created or shared to deceive.

Online Exploitation

Abuse or manipulation that takes place through digital technology for sexual, criminal or financial gain.

Aims

Esland Online School is committed to creating a safe, supportive and empowering digital environment in which pupils can learn, communicate and develop the knowledge and skills required to navigate an increasingly online world. We recognise that technology provides significant opportunities for learning, creativity and connection, but also presents risks that require a proactive and safeguarding-led response.

Our approach to online safety seeks to protect and educate the whole school community. We aim to develop pupils' understanding of online risk, promote positive and respectful behaviour in digital spaces, and ensure that robust systems are in place to identify, respond to and manage concerns effectively. Through education, partnership with families and strong safeguarding practice, we seek to build digitally resilient young people who are able to participate safely and confidently in online environments.

The 4 key categories of risk

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

Content – being exposed to extremist material, pornography, self-harm content, suicide content, hate speech, misinformation and disinformation

Contact – being subjected to harmful online interactions including grooming, exploitation, radicalisation, online coercion and sextortion

Conduct – personal online behaviour that increases the likelihood of cyberbullying, sharing inappropriate content, online harassment, making and sharing nudes/semi-nudes and misuse of technologies

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams, and fraud

Child-on-Child Online Harm

The school recognises that online harm can occur between children and may include cyberbullying, harassment, sexual harassment, image-based abuse, coercive behaviour, exploitation, hateful content and the sharing of nude or semi-nude images. All concerns involving child-on-child abuse are managed in accordance with the Child Protection and Safeguarding Policy and will be addressed using a safeguarding rather than solely behavioural response.

Roles and Responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge

to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Governing Body has strategic responsibility for online safety and receives regular assurance regarding the effectiveness of safeguarding arrangements, staff training, filtering and monitoring systems, and emerging risks.

Governors provide challenge and oversight to ensure that online safety remains a key component of safeguarding practice across the school.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher will:

- Lead implementation of this policy.
- Ensure staff training is completed.
- Ensure safeguarding arrangements are effective.
- Review online safety incidents.
- Report significant concerns to governors.

The designated safeguarding lead (DSL)

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

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The IT manager

The IT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a frequent basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, 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 school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the IT Manager, Education Director and the Headteacher.
- Following the correct procedures by contacting IT Manager, Education Director and the Headteacher. if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school 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.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers 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](#)
- Parent resource sheet – [Childnet](#)

Visitors and members of the community

Visitors and members of the community who use the school'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 (appendix 3).

Online Learning Environment Safeguarding

Esland Online School recognises that safeguarding within virtual learning environments is central to the safety and wellbeing of pupils. As a fully online provision, we acknowledge that risks may present differently to those found in traditional educational settings and therefore require specific approaches to supervision, communication and professional conduct.

All teaching and learning activities take place through approved school platforms and are subject to the same safeguarding expectations as face-to-face education. Staff maintain professional boundaries at all times and communicate with pupils only through authorised school systems. Pupils are expected to engage respectfully and responsibly in live lessons, online discussions and all digital communication.

The school has procedures in place to ensure that online lessons, individual support sessions and electronic communications are delivered safely and transparently. Any safeguarding concerns identified through lesson participation, pupil presentation, online interactions or communication with staff are managed in accordance with safeguarding procedures and recorded appropriately.

Filtering and Monitoring

Esland Online School maintains filtering and monitoring arrangements that are proportionate to the needs of pupils and compliant with current Department for Education expectations. These arrangements form part of the school's wider safeguarding systems and are designed to support safe access to technology whilst enabling effective teaching and learning.

The school uses filtering systems to reduce the risk of children accessing harmful, inappropriate or illegal content and monitoring systems to identify behaviours or activity that may indicate safeguarding concerns. Monitoring information is reviewed by appropriate members of staff and any concerns are managed through the school's safeguarding procedures. The effectiveness of filtering and monitoring arrangements is reviewed regularly alongside emerging technologies, changing risks and updates to statutory guidance. Staff receive training on their responsibilities and understand how to report concerns regarding the effectiveness of these systems

Monitoring arrangements include:

- Website access, platform and search activity monitoring using Senso
- Safeguarding alerts via Smoothwall
- Incident review processes.

Requests to bypass filtering systems must:

- Be educationally justified, approved by senior leaders and recorded for audit purposes.

Artificial Intelligence (AI)

Esland Online school recognises that artificial intelligence is increasingly becoming part of everyday life and education. AI technologies offer opportunities to support learning, creativity and productivity, but also present emerging safeguarding, ethical and educational risks.

The school promotes the safe, critical and responsible use of AI. Pupils are taught to evaluate AI-generated content carefully, recognise misinformation and manipulated media, understand the limitations of AI systems and consider the ethical implications of their use. Particular attention is given to emerging risks such as deepfakes, impersonation, online exploitation and the spread of misleading information.

Where staff choose to utilise AI technologies to support professional practice, they remain professionally accountable for the content they produce and use. Confidential information, personal data and safeguarding information must never be entered into publicly available artificial intelligence platforms. The use of AI within teaching, learning and administration must always align with safeguarding, data protection and professional standards.

Staff may make appropriate use of approved artificial intelligence tools to support teaching, planning, administration and professional practice. However, they remain professionally responsible for any content produced or used and must ensure that all information is accurate, appropriate and compliant with safeguarding and data protection requirements. Personal data, confidential information and safeguarding records must never be entered into publicly available AI platforms.

Through the curriculum, pupils are supported to understand both the opportunities and limitations of artificial intelligence. This includes developing an understanding of ethical use, academic integrity, deepfakes, misinformation, manipulated media and the responsible use of emerging technologies. Any misuse of artificial intelligence, including impersonation, harassment, cyberbullying or the creation of harmful content, will be managed through the school's safeguarding and behaviour procedures.

Educating pupils about online safety

The Esland Online School operates on a "Stage not Age" approach to education. Whilst the Esland Online School will not place KS1 and KS2 aged children, it is imperative that knowledge from these Key Stages is implemented into the curriculum.

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of the primary school stage**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- How to report a range of concerns

By the **end of the secondary school stage**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for our vulnerable children, victims of abuse and some pupils with SEND.

Supporting vulnerable pupils

Esland Online School recognises that online risk is not experienced equally and that many of our pupils may face additional vulnerabilities when accessing digital environments. Pupils with social, emotional and mental health needs, autism, developmental trauma, communication differences or previous adverse experiences may require additional support to recognise risks, establish boundaries and seek help when concerns arise.

The school therefore adopts a personalised and therapeutically informed approach to online safety education. Support is adapted according to developmental readiness, individual need and identified risk rather than chronological age alone.

Online safety forms part of wider safeguarding, pastoral and therapeutic planning and reflects the school's commitment to understanding each child as an individual.

Educating parents/carers about online safety

We recognise that parents and carers play a crucial role in supporting children to stay safe online. The school works collaboratively with families to promote safe, responsible and positive engagement with technology. Online safety information, advice and resources are shared regularly through school communications, meetings and information events. Where concerns arise, the school seeks to work in partnership with parents and carers to ensure that risks are understood and managed effectively.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Acceptable use of internet during school hours, whilst at home

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3).

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school'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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Acceptable use of the internet outside of school hours

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3).

Use of the 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, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

Staff using work devices outside school

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 that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT manager and Education Director.

Social Media and Professional Conduct

All members of staff are expected to maintain appropriate professional boundaries and exercise good judgement when using social media, electronic communication and digital technology. Staff should be mindful that their online conduct may affect pupils, colleagues, parents and the reputation of the school.

Communication with pupils must take place only through approved school systems and in line with safeguarding procedures. The school expects all staff to model safe, respectful and responsible online behaviour and to comply with the Staff Code of Conduct, Data Protection Policy and safeguarding requirements at all times.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on IT and internet 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 school'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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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, threatening, 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.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

Monitoring Arrangements

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

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available [here](#)) 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.

Appendix 1 Acceptable use agreement (pupils and parents/carers)

At Esland Online School, technology is at the heart of our learning community. We want all pupils to feel safe, respected and supported when learning online. This agreement sets out the expectations for using school systems, participating in online lessons and communicating with others. By working together, we can ensure that online learning remains a positive experience for everyone. .

Pupil Agreement

When I access Esland Online School systems, attend online lessons or communicate with staff and other pupils, I agree to:

- Use school technology and online platforms responsibly and for learning purposes.
- Treat other people with kindness, respect and consideration at all times.
- Follow the instructions and expectations set by staff during live lessons and online activities.
- Use appropriate language, images, profile names and communication.
- Keep my usernames and passwords secure and not share them with anyone else.
- Protect my personal information and the personal information of others.
- Tell a trusted adult or member of staff if I see or experience something online that makes me feel uncomfortable, worried or unsafe.
- Respect other people's privacy and wellbeing when communicating online.

I understand that I must not:

- Bully, threaten, harass or intentionally upset another person online.
- Share inappropriate, offensive, discriminatory or harmful content.
- Pretend to be someone else online.
- Access material that is illegal, harmful or inappropriate.
- Share confidential school information without permission.
- Record lessons, take screenshots, save images or share content from lessons without authorisation from the school.
- Use artificial intelligence tools to complete work dishonestly or present AI-generated work as my own.
- Deliberately disrupt lessons or interfere with the learning of others.

Participation in Online Lessons

To help create a safe and productive learning environment, I understand that:

- I should attend lessons regularly and engage positively in learning.
- I should join lessons using the school-approved platform and account.
- I should communicate respectfully through microphones, cameras and chat functions.
- I should participate from an appropriate location wherever possible.
- Any concerns about my safety or wellbeing observed during lessons may be shared with safeguarding staff in line with the school's safeguarding procedures.

Artificial Intelligence (AI)

I understand that AI tools can be useful for learning, but I must use them responsibly. If I use AI to support my learning, I will be honest about this and follow instructions given by staff. I will not use AI to mislead others, create harmful content, impersonate another person or gain an unfair advantage in my learning.

Monitoring and Safeguarding

I understand that Esland Online School may monitor the use of school systems, platforms and online activity to help keep pupils safe. This monitoring forms part of the school's safeguarding responsibilities and helps staff respond to concerns where necessary.

Pupil Declaration

I have read, discussed and understood this agreement. I understand that if I do not follow these expectations, the school may take action in line with its behaviour, safeguarding and online safety policies.

Pupil Name: _____

Pupil Signature: _____

Date: _____

Parent/Carer Agreement

As a parent/carers, I recognise the importance of online safety and will support my child to use technology safely, responsibly and respectfully.

I will:

- Encourage my child to follow this agreement.

- Support the school's online safety expectations.
- Raise any concerns about online safety or wellbeing with the school promptly.
- Help my child understand how to stay safe online.
- Work in partnership with the school where concerns arise.

I understand that the school may monitor activity on its systems and online learning platforms as part of its safeguarding responsibilities, and that information may be shared with appropriate professionals where there are concerns about a child's safety or wellbeing.

I have read and understood this agreement and will support my child to follow it.

Parent/Carer Name: _____

Signature: _____

Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors

Technology is central to the teaching, learning and safeguarding arrangements at Esland Online School. All staff, governors, volunteers and visitors have a responsibility to model safe, respectful and professional online behaviour and to contribute to a culture in which pupils feel safe, supported and able to learn.

This agreement outlines the expectations for the use of school technology, communication systems and online learning environments. It should be read alongside the Online Safety Policy, Safeguarding and Child Protection Policy, Data Protection Policy and Staff Code of Conduct.

Professional Conduct

As a member of the Esland Online School community, I understand that my conduct online should reflect the same professional standards expected in any face-to-face educational environment. I will maintain appropriate professional boundaries at all times and recognise that online interactions with pupils are subject to the same safeguarding expectations as any other professional relationship.

I will communicate with pupils and families only through approved school systems and authorised communication channels. I will not use personal social media accounts, personal email addresses, messaging services or personal telephone numbers to communicate with pupils unless this has been explicitly approved through school procedures.

I understand that my online behaviour, including my use of social media, may affect the reputation of the school and the confidence that pupils, families and colleagues place in me as a professional.

Safeguarding Responsibilities

I recognise that online safety is a safeguarding responsibility and that concerns arising from online interactions, pupil behaviour, digital activity or online content must be treated as safeguarding matters where appropriate.

I understand that concerns relating to child-on-child abuse, online sexual harassment, image-based abuse and the sharing of nude or semi-nude images are safeguarding concerns and must be managed in accordance with safeguarding procedures.

I will:

- Remain alert to signs of online abuse, exploitation, grooming, radicalisation, bullying, harmful sexual behaviour or other forms of online harm.
- Report concerns promptly in line with safeguarding procedures.
- Record concerns accurately and objectively.
- Follow school procedures when responding to safeguarding incidents online.
- Maintain an attitude of "it could happen here" when considering online safety concerns.

Use of Online Learning Platforms

When delivering or supporting online learning, I will use only approved school platforms, systems and accounts.

I will ensure that:

- Online sessions are conducted in a professional, transparent and appropriate manner.
- Electronic communications remain professional and relevant to education and safeguarding purposes.

- Pupils are treated with dignity, respect and consistency.
- Any concerns identified during live lessons, one-to-one sessions or digital communications are reported and recorded appropriately.
- School procedures relating to lesson recording, storage of information and safeguarding oversight are followed.

Information Security and Data Protection

Staff understand that all personal data must be processed lawfully, fairly and transparently in accordance with UK GDPR and the Data Protection Act 2018. Information should only be accessed where there is a legitimate professional purpose and must not be retained, downloaded, printed or shared unnecessarily.

I understand my responsibility to protect confidential information and personal data.

I will:

- Keep usernames and passwords secure.
- Ensure school devices are protected appropriately.
- Access only information required for my role.
- Store and share information in accordance with data protection requirements.
- Report any actual or suspected data breaches immediately.

I will not:

- Share confidential information inappropriately.
- Allow unauthorised individuals access to school systems.
- Store sensitive information on unauthorised devices or systems.
- Access, alter or share information I am not authorised to use.

Artificial Intelligence

Esland Online School recognises the opportunities and risks associated with artificial intelligence technologies.

Where I use approved AI tools to support planning, administration or teaching, I remain professionally accountable for the content produced and how it is used. I will critically evaluate any AI-generated content before using it and ensure it is accurate, appropriate and suitable for the intended purpose.

I understand that safeguarding information, personal data, confidential pupil information and commercially sensitive information must never be entered into publicly available artificial intelligence platforms.

I will promote the ethical, safe and responsible use of AI and support pupils to develop an informed understanding of both the opportunities and risks associated with emerging technologies.

Monitoring and Filtering

I understand that the school operates filtering and monitoring systems as part of its safeguarding arrangements. These systems support the protection of pupils, staff and school systems and help identify concerns that may require intervention.

I will work within these systems and follow appropriate procedures if educational activities require access to resources that would normally be restricted.

Personal Devices and Remote Working

When working remotely or using school devices away from my usual place of work, I will take reasonable steps to maintain security and confidentiality. This includes ensuring devices are password protected, software is kept up to date, information is stored securely and screens cannot be viewed by unauthorised individuals.

Where personal devices are used for work purposes, I will ensure they meet the school's expectations regarding security, confidentiality and data protection. Sensitive pupil information will not be stored locally on personal devices unless specifically authorised and protected in accordance with school procedures.

Declaration

I have read and understood this Acceptable Use Agreement and agree to comply with its requirements at all times. I understand that failure to do so may result in action being taken in accordance with the school's policies and procedures. I confirm that I have read and understood the Online Safety Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct, Data Protection Policy and guidance relating to the safe use of artificial intelligence technologies.

Name: _____

Role: _____

Signature: _____

Date: _____

Appendix 3 Online safety training needs – self-audit for staff

online safety training needs audit	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	