Ladygrove Primary School and Nursery

Online Safety and Acceptable Use Agreement

January 2026

To be reviewed: January 2027

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

This advice brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach.

Refer to the education for a connected world framework for age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

DFE Teaching Online Safety in Schools January 2023

Contents

1. Introduction 1
2. Responsibilities 1
3. Scope of policy 1
4. Policy and procedure
    - Visiting online sites and downloading 2
    - Storage of Images 4
    - Use of personal mobile devices (including phones) 4
    - Reporting incidents, abuse and inappropriate material 5
5. Curriculum 5
6. Staff and Governor Training 6
7. Working in Partnership with Parents/Carers 6
8. Records, monitoring and review 7
9. Appendices of the Online Safety Policy 7

Appendix A -Online Safety Acceptable Use Agreement - Staff ,Governors,student teachers 8

Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches and supply teachers 11

Appendix C - Requirements for visitors, volunteers and parent/carer helpers 14

Appendix D - Online Safety Acceptable Use Agreement Primary Pupils 15

Appendix E - Online safety policy guide - Summary of key parent/carer responsibilities 19

Appendix F - Guidance on the process for responding to cyberbullying incidents 20

Appendix G - Guidance for staff on preventing and responding to negative comments on social media 21

Appendix H - Online safety incident record 25

1. Introduction

Ladygrove Primary School and Nursery recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play whilst understanding the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all pupils, staff and governors** will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

Emotional health and welling linked with Computing

Here at Ladygrove Primary School and Nursery, we see children's emotional wellbeing as being just as important as their physical health. Good mental health helps pupils to **develop the resilience to cope** with whatever life throws at them and grow into well-rounded, healthier, happier adults. We want children to recognise that through learning we make mistakes and mistakes help us to grow.

Staff are aware that certain areas of online safety may cause anxiety and all matters of a sensitive nature will be addressed as such. Any pupils deemed to be affected on certain subjects will be identified and given support immediately.

KCSIE 2025 Update – Emerging Technologies and Digital Safeguarding

The school recognises the rapidly changing nature of technology, including the increased use of artificial intelligence, image-generation tools, online algorithms and cross-platform communication. In line with KCSIE 2025, the school will ensure pupils are taught how to identify manipulated or AI-generated content, understand the risks associated with fake profiles or altered images, and recognise how persuasive design and algorithms influence what they see online. Staff will remain vigilant to the ways emerging technologies may be used to bully, exploit or mislead pupils, and will report concerns through safeguarding channels.

In the world of social media, there is a significant amount of research that shows mental health and wellbeing can be affected negatively. We want children to recognise how useful technology is in terms of education and communication, but we also want them to use it responsibly.

2. Responsibilities

The headteacher, Deputy Headteacher (Online Safety Lead) and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named Computing Coordinators in this school are Max Trusler and Lucy Taffinder.
All breaches of this policy must be reported to Kirsty Stewart (Online safety lead)
All breaches of this policy that may have put a child at risk must also be reported to the Designated Safeguarding Lead, Kirsty Stewart

KCSIE 2025 Update – Digital Risk Oversight
The Online Safety Lead and DSL will ensure that all digital tools, platforms, applications and online communication systems used within the school are risk-assessed prior to use. Digital safeguarding risk assessments will consider risks relating to contact, conduct, content and contract, as well as emerging risks such as AI-manipulated images, identity spoofing and cross-platform messaging. Governors must receive clear monitoring reports which demonstrate ongoing oversight of online safety practice, filtering, monitoring and staff training.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

KCSIE 2025 Update – Family Awareness
Parents/carers should be aware of the increased risks associated with AI-generated content, including manipulated photos, anonymous messaging and impersonation. Families should encourage children to discuss anything that appears unusual, unrealistic or worrying online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents:

- Safeguarding
- Keeping Children Safe in Education
- GDPR
- Health and safety
- Home–school agreement
- Home learning
- Behaviour
- Anti-bullying
- PSHE/RSE policies
- Mobile phone and smart watch policy

- Online safety risk assessment
- Filtering and Monitoring

4. Policy and procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

KCSIE 2025 Update – Digital Safeguarding Standards

The school will maintain a whole-school approach to online safety. Online safety will be embedded across safeguarding practice, staff training, teaching and learning, leadership responsibilities and parental engagement. Staff must understand how online behaviour can escalate into offline risk and must report all concerns immediately.

The school expects everyone to use internet, mobile and digital technologies responsibly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher.

- When working with pupils who are searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

KCSIE 2025 Update – AI-Generated and Manipulated Content

Staff must be aware that technology can produce AI-generated images, videos and messages that appear realistic. Any discovery or disclosure involving manipulated or deepfake content relating to a pupil or staff member must be treated as a safeguarding concern and reported immediately to the Online Safety Lead or DSL.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Use the school's hardware and Wi-Fi facilities for running a private business
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by Computing Coordinator: Max Trusler. For example, child safety educational content/ workshops for children.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by Jo Weichlbauer and Kirsty Stewart.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

KCSIE 2025 Update – Image Security and AI Misuse

No pupil or staff images will be uploaded to any platform that uses facial-recognition, machine learning or AI-training mechanisms without explicit consent and a completed digital risk assessment. Staff must remain aware that images can be digitally manipulated or reused without permission; any concerns about photo misuse must be reported and logged on CPOMS.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Jo Weichlbauer or Kirsty Stewart. When a parent/carer is on school premises their phone/s must be either left in the car or locked away in a locker and they will keep the key on them.

Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. Mobile devices/phones must be given to the reception staff to be securely locked away during school hours. All such devices must be switched off during this time. Under no circumstance should pupils use their personal mobile devices/phones to take images of

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.

KCSIE 2025 Update – Cross-Platform Contacts

KCSIE 2025 highlights increased risks relating to cross-platform communication (e.g., gaming chats, social media messaging, voice notes, and anonymous messaging services). Staff must remain vigilant to reports from pupils involving communication with unknown individuals, or the use of platforms not recommended for primary age children. All such concerns must be escalated to the DSL.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the headteacher or deputy headteacher. All online safety disclosures will be reported on CPOMS. Where such an incident may lead to significant harm, safeguarding procedures should be followed. Where judged necessary, Kirsty Stewart will refer details to social care or the police.

KCSIE 2025 Update – Harmful and Manipulated Digital Content

Any incident involving AI-generated bullying, identity impersonation, the sharing of manipulated images, or the use of online tools to threaten, coerce or intimidate must be recorded on CPOMS and escalated. Staff must not attempt to view or save harmful content; the principle of minimal handling applies.

5. Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum , Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism,

understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

- How the law can help protect against online risks and abuse

KCSIE 2025 Update – AI, Manipulation & Digital Literacy

The curriculum will include explicit teaching about: AI-generated content and deepfake risks; recognising manipulated or misleading online information; understanding algorithmic bias and targeted content; identifying commercial manipulation such as loot boxes, gambling-style mechanics and scams; reporting concerns about identity misuse, impersonation or AI-generated bullying; and navigating persuasive online design features safely.

6. Staff and Governor Training

Staff and governors are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

KCSIE 2025 Update – Staff Competency in Digital Safeguarding

All staff training will include recognising AI-manipulated content; understanding risks associated with image-generation and impersonation; safe use of AI-enabled tools; handling digital evidence safely; and identifying grooming, coercion and radicalisation that begins online or via gaming platforms. Training records will reflect these additions as part of safeguarding compliance.

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in Appendix E. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

KCSIE 2025 Update – Termly Filtering Oversight

Filtering and monitoring systems will be reviewed termly by senior leaders and governors. Records will include: categories blocked and allowed; incidents triggered; actions taken; and outcomes of digital risk assessments. Governors will receive detailed termly updates showing the effectiveness of filtering and monitoring arrangements.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)

KCSIE 2025 Update

All acceptable use expectations now include responsibilities relating to AI-generated content, deepfakes, impersonation, and manipulated images or messages. Any concerns relating to these risks must be reported immediately to the Online Safety Lead or DSL.

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

KCSIE 2025 Update – Digital Safeguarding Responsibilities

All staff must understand risks associated with emerging technologies, including AI-generated content, identity manipulation, impersonation and deepfake material. Any concerns must be treated as a safeguarding issue and reported immediately to the Online Safety Lead or DSL.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff , student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Max Trusler. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to Kirsty Stewart and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

KCSIE 2025 Update – Safe and Approved Use of AI

Staff must recognise that AI tools may generate biased, harmful or misleading content. Use of AI platforms involving pupil data, pupil images or messages must not take place without formal approval and a completed digital risk assessment.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Kirsty Stewart.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing body
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

KCSIE 2025 Update – Manipulated Images

Staff must be vigilant to the risk of images being digitally altered or misused. Any suspicion that pupil or staff images have been manipulated or shared without consent must be reported.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding

allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Max Trusler

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSL or Kirsty Stewart.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Kirsty Stewart.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership ,DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature …….…….…… Date ……

Full Name ……..... (printed)

Job title ……

Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

School name

Online safety lead

Designated Safeguarding Lead (DSL)

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

KCSIE 2025 Update – Visiting Staff Responsibilities

All visiting staff must recognise digital safeguarding risks including AI-generated impersonation, manipulated images and cross-platform messaging. Any concerns must be escalated immediately.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with Kirsty Stewart. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Kirsty Stewart

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with Kirsty Stewart

Social networking

I understand the need to separate my professional role from my private friendships; in my professional

capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil’s or parent/carer devices can be used, with parent/carer agreement.

KCSIE 2025 Update – External Platforms

Digital images must not be uploaded to any platform that uses AI-training mechanisms without explicit school consent. Staff must not use apps with unverified data-processing practices.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher’s personal device. Recordings can be made with the child’s and parent/carer’s agreement on a school device, an organisational device approved by the headteacher/DSL, or a young person’s or parent/carer’s own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Max Trusler.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL or Kirsty Stewart.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Kirsty Stewart.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..……..……..…… Date ……..……

Full Name ……..... (Please use block capitals)

Job Title/Role ……..……..……

Appendix C - Requirements for visitors, volunteers and parent/carer helpers

KCSIE 2025 Update

All acceptable use expectations now include responsibilities relating to AI-generated content, deepfakes, impersonation, and manipulated images or messages. Any concerns relating to these risks must be reported immediately to the Online Safety Lead or DSL.

(Working directly with children or otherwise)

School name……..…...

Online safety lead ……..……

DSL ……..…..

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

KCSIE 2025 Update – Visitor Awareness

Visitors must report any concerns relating to harmful online behaviour, including suspected image manipulation, impersonation or any digital content that may put a child at risk.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSL

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Devices will be stored in a lockable container at the office. Any exception must be pre-arranged.

KCSIE 2025 Update – Emerging Risks

Visitors should be aware that emerging online risks such as deepfake content, fake profiles and coercive messaging may impact children. Any concerns must be shared immediately with the DSL or headteacher.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSL or headteacher is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about pupils,

staff, school systems and plans. Such information should never be shared on line, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.

- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix D - Online Safety Agreement Primary Pupils

My online safety agreement

- I will ask permission before using digital technologies and/or software (including Purple Mash, Times Table Rockstars and Natterhub).
- I will keep my password private.
- I will log out when not using digital technologies and/or software (including Purple Mash, Times Table Rockstars and Purple Mash).
- I will ask permission before taking photos of people and uploading them onto any device or online service (including Natterhub and Purple Mash).
- I will create content for positive reasons.
- I will support my classmates and report negative comments.
- I will check the timer whilst using online platforms and ensure I do not excessively use the online platforms (including Natterhub and Purple Mash).
- I know that poor choices will result in my screen time being reduced or accounts temporarily locked or permissions removed.
- I know that all games, platforms and software have age restrictions to keep me safe.
- I agree to all the above terms.

Dear Parent/Carer,

KCSIE 2025 Pupil Update
Pupils will also learn how to: recognise altered, fake or AI-generated images; report fake profiles or people pretending to be someone else; understand that some online content is designed to trick, mislead or manipulate; and tell an adult if they see content that feels “not real”, confusing, or worrying.

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with Mr Trusler or Mrs Stewart.

Please return the signed sections of this form which will be kept on record at the school.

<u>Pupil agreement</u>

Pupil name……..…

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature……..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and stored either in a vehicle or in a locker at reception.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)……

Parent/carer signature……..

Date ……..…..…

Appendix E - Online safety policy guide - Summary of key parent/carer responsibilities

KCSIE 2025 Update

All acceptable use expectations now include responsibilities relating to AI-generated content, deepfakes, impersonation, and manipulated images or messages. Any concerns relating to these risks must be reported immediately to the Online Safety Lead or DSL.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.

KCSIE 2025 Update – No AI-Generated Media
Parents must not use or share AI-generated images or videos of pupils or staff under any circumstances.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix F - Guidance on the process for responding to cyberbullying incidents

KCSIE 2025 Update

All acceptable use expectations now include responsibilities relating to AI-generated content, deepfakes, impersonation, and manipulated images or messages. Any concerns relating to these risks must be reported immediately to the Online Safety Lead or DSL.

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

KCSIE 2025 Update – New Forms of Digital Harm

KCSIE 2025 highlights new forms of digital harm including AI-generated bullying (e.g., fake images/messages), identity misuse or impersonation, sharing of altered images, and coercive messaging using anonymous services or gaming platforms.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.

KCSIE 2025 Update – Minimal Handling of Harmful Content

Staff must not attempt to view deepfake or manipulated sexualised images. These must be reported immediately to the DSL and police.

- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

KCSIE 2025 Update

All acceptable use expectations now include responsibilities relating to AI-generated content, deepfakes, impersonation, and manipulated images or messages. Any concerns relating to these risks must be reported immediately to the Online Safety Lead or DSL.

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix E (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

KCSIE 2025 Update – Misleading Digital Content

Schools should consider the impact of AI-generated or altered posts that may falsely portray the school, staff or pupils. Any such content must be reported and dealt with following safeguarding and legal guidance.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

KCSIE 2025 Update – False Portrayals

Senior staff should also consider whether AI-generated content has been used to mislead or harm the school community and act accordingly.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any

evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to reiterate the seriousness of the matter.

Appendix H ONLINE Risk Assessment

Safeguarding risk assessment online	
Audience:	Staff who want to provide an online/mobile social media or interactive service (e.g. online lessons, a social network, messaging, Q&A site, interactive game,cloud service or ephemeral messaging service) to users who are under 18 years old.
Purpose:	The primary objective of this tool is to protect children from online risk by enabling staff to self-assess online products/services and inform them of mitigationstrategies which must be put in place to reduce the risk of harm to children.
Online Risks:	**Online risk can be classified in FOUR ways: THE 4 C's**
	Conduct risk: children participating in an interactive situation. This includes bullying, sexting, harassing, being aggressive or stalking; or promoting harmfulbehaviour such as self-harm, suicide, pro-anorexia, bulimia, illegal drug use or imitating dangerous behaviour. A child's own conduct online can also make them vulnerable - for example, by over-sharing their personal information or by harassing or bullying others.
	Contact risk: children being victims of interactive situations. This includes being bullied, harassed or stalked; meeting strangers; threats to privacy, identityand reputation (for example, through embarrassing photos shared without permission, a home location being identified, someone impersonating a user, users sharing information with strangers); and violence, threats and abuse directly aimed at individual users and/or groups of users.
	Content risk: children receiving mass-distributed content. This may expose them to age-inappropriate material such as pornography, extreme violence, orcontent involving hate speech and radicalisation.
	Contract risk: children are party to and/or exploited by a potentially harmful contract. A child as a consumer can be exposed to identify theft, phishing scams , gambling and blackmail
Illegal contact, conduct, content and contract	**Some online risks cannot only lead to harm, but also result in illegal activity such as:**
	** sexual grooming and sexual exploitation*
	** creation and distribution of child abuse images*
	** online aspects of child trafficking*
	** online radicalisation*
	** physical and mental abuse of children*
	** selling and distributing illegal drugs*
	** revenge pornography, harassment and malicious communications.*
Core Principles:	**1. Informed parental consent**
	2. Educating and raising awareness of e-safety
	3. Effective moderation

	4. Ensuring privacy and controls
	5. Dealing with child sexual abuse content and other illegal contact
	6. Managing inappropriate or harmful content
	7. Dealing with inappropriate or harmful behaviour

Appendix I

	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Filtering and Monitoring

Internet filtering and monitoring is managed by our network service provider, Telford and Wrekin Council.

Telford & Wrekin COUNCIL

The web and content filtering system used is Lightspeed Systems. The school can request access to a blocked website if the risks are deemed safe.

Lightspeed Systems®

Senso is a web-based system set up by T&W and managed within school. This takes screenshots of any trigger words and is compiled into a weekly report which is sent to both the Headteacher and Deputy headteacher. Staff and pupils' screens can be monitored through remote access to desktops. Trigger words, set by T&W and amended by the school, are reviewed regularly to check their relevance and importance – especially if there is a series of false positive reports of a particular word.

senso.cloud
www.senso.cloud

Training of the monitoring and filtering system is given to relevant staff and passed on to all staff through safeguarding updates.

SOPHOS

Sophos is used to filter emails for protection against spam and viruses.

At Ladygrove, Kirsty Stewart (Deputy headteacher) is the online safety lead. This is also monitored by Jo Weichlbauer (Headteacher). They manage the situation in line with the Child Protection and Safeguarding policy and Keeping Children Safe in Education.

Appendix K: Example Online safety Newsletter for parents and carers

Knowsley City Learning Centres

Online Safety Newsletter March 2024

Managing Screen time from Internet Matters

Are you worried your child has too much screentime or would like more advice on how to support your child in managing their screen time? Internet Matters have a wealth of information on their website to help support you.

This first link discusses how to get the most out of screen time and how to talk to your child about screen time based on their age:

- https://www.internetmatters.org/issues/screen-time/protect-your-child

This second link provides advice on how to tackle too much screen time and what the signs of too much screen time might be:

- https://www.internetmatters.org/issues/screen-time/deal-with-it/

This final link provides a guide on how to balance screen time:

- https://www.internetmatters.org/resources/creating-a-balanced-digital-diet-with-screen-time-tips/



Fortnite Battle Royale

Fortnite Battle Royale is rated PEGI 12 because it features moderate violence which means it is not suitable for persons under 12 years of age.

It is important to remember that when rating games, PEGI do not take into consideration the communication features of a game. Fortnite does include a chat facility, which adds further risks.



What is Fortnite?

There are different versions of Fortnite, including Battle Royale, which is free to play (although in-app purchases are available). In Battle Royale up to one hundred players compete against each other.

What do I need to be aware of?

- **Chatting to strangers and inappropriate language:** Fortnite contains voice and text chat. Due to the nature of the game, your child may be chatting to strangers and may hear inappropriate language. Ensure your child knows how to report players for any inappropriate behaviour.
- **In app purchases:** All users can purchase V-Bucks directly through the game so make sure you don't store your card details within the game/device and restrict purchases.

Parental Controls

Fortnite includes several parental controls to help you make it a safer environment for your child including disabling voice chat, filtering language and setting privacy settings. **Also, remember to set up age-appropriate parental controls on the device your child is playing on.**

Further information

Virgin Media outline how to set up the different parental controls available: https://www.virginmedia.com/blog/parental-controls/gaming-fortnite

Does your child need a mobile phone?

If you are thinking about giving your child their own phone, then you might find this article from Family Lives useful as it discusses things you need to consider:

https://www.familylives.org.uk/advice/primary/health-and-development/does-your-child-need-a-mobile-phone

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date released 01.03.24.

Instagram

You will probably know that Instagram is used to post photos and videos, but did you know that it can also be used to message, voice/video call and send disappearing messages? Users can also upload to 'Stories' (which disappear after 24 hours), broadcast live and upload reels (short videos).

You must be over 13 years of age to set up an account. To create an account, you must enter a date of birth (but it is not verified). *When you set up an account for users under 16 years old, the account is set to Private. This is the recommended setting so that your child approves who follows them and sees their content.* Even if your child's profile is private, their bio (at the top of their profile) can still be seen by **everyone.** Check they have not included personal information here e.g. they should not be wearing their school uniform in their photo.

Instagram includes several privacy settings, so go through these with your child and ensure they are set appropriately. Settings include:

- Messages/Group chats – set who can message you/add you to groups.
- Story replies – you can turn this off or choose who can message you.
- Hidden words – turn this option on to hide comments/messages that may be offensive. You can also add your own custom words or emojis.

Make sure your child understands that there is a risk that content they upload can be shared with others without their permission as other users can screenshot it.

Supervision

You can set up supervision on your child's (aged 13-17) Instagram account. This gives you access to a set of tools including the ability to see who they follow/who follows them, how much time they are spending on Instagram, set a time limit and view accounts your child has blocked. Your child can also share when they have reported anything to Instagram with you. Learn more here: https://help.instagram.com/658522825492278

Safety Features

Ensure your child knows how to report posts and people, how to unfollow and block people, delete and turn off comments. View here: https://help.instagram.com/269765046710559

Quiet mode

Your child can activate quiet mode, so they do not receive notifications (to provide less distraction whilst studying and at night time).

How can I keep my child safe on Instagram?

The NSPCC have published a blog with everything that you need to know: https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-safety-blog/keeping-children-safe-on-instagram/

More information

- Visit the family centre to learn more about the features available: https://familycenter.instagram.com/
- Download a parent's guide to Instagram: https://help.instagram.com/299484113584685

Do you need help managing your child's device?

You can use Google Family Link or Apple Family Sharing to help you depending on your child's device.

Google Family Link

This is a parental control app from Google that lets you:
- See activity reports showing how long they spend on each app.
- Approve or block new app downloads.
- Set screen time limits.
- Find their location (using their device).

You will need to download an app and then decide appropriate settings.

https://families.google.com/familylink

Apple Family Sharing

You can set up Family Sharing in the settings of your device. Family Sharing allows you to:
- Share Apple subscriptions.
- Share purchases from the App Store.
- Approve what children purchase/download.
- Limit screen time.
- Share locations and find devices.

https://www.apple.com/uk/family-sharing/

Monitoring Apps (paid for)

In addition, there are apps that you can pay for that you may find provides a better solution for you. Whilst we cannot recommend a specific product, these are some examples that you could review and test using a free trial:

- Norton Family: https://uk.norton.com/products/norton-family
- Qustodio: https://www.qustodio.com/en/
- Family Time: https://familytime.io/



Appendix L: Pupil team 'Digital Leaders' Online safety poster

Policy- Document Status			
Date of Policy Creation	**March 2022 – reviewed every year annually**	**Named Responsibility**	M Trusler E Guess
Date of review completion	**January 2026**	**Named Responsibility**	Pupils, Staff, Parents and Governors
Inception of new Policy	**January 2026**	**Named Responsibility**	Kirsty Stewart Max Trusler
Date of Policy Adoption by Governing Body		**January 2026**	