LOCHINVER HOUSE

Online Safety Policy

Contents

Introduction 1
Aims of this Policy 2
Curriculum and Tools for Learning 2
Early Years Use of Mobile Phones, Cameras and Devices with Imaging and Sharing Capabilities 3
Email 3
Filtering and Monitoring Safeguarding Measures 3
Incident Reporting 3
Monitoring 4
Online sites and downloading 4
Parents and Visitors 5
Personal mobile devices (including phones) 5
Pupils 6
Social Media 6
Staff 7
Storage of Images 7
Video and Photography at School Events 7
Visitors and Visiting Speakers 8
The School's Responsibilities 8
Appendix 1 - Procedures in the Event of a Breach of this Policy 9
Appendix 2 – Incident Reporting Form 10
Appendix 3 – Online Safety Agreement for Pupils in Early Years and Year 1 11
Appendix 4 – Online Safety Agreement for Pupils in Years 2 – 4 12
Appendix 5 – Online Safety Agreement for Pupils in Years 5 – 8 13
Appendix 6 – Pupil-Parent iPad Use Agreement 14
Appendix 7 – Mobile Phone Agreement – Pupils 15

Introduction

Lochinver House School recognises that internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. This policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school-based devices, the internet, email, instant messaging and other social networking technologies and mobile phones and games, to safeguard adults and pupils. This policy details how the School will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable use or misuse of these technologies by adults or pupils.

This policy is supported by our Child Protection and Safeguarding Policy and Procedure (incorporating Staff Behaviour and Code of Conduct), applies to everyone and is intended to protect the interests and safety of the whole School Community. It is also applicable to partners and other providers in circumstances where pupils who receive part of their education off site or who are on a School trip to ensure they remain safe online.

Online Safety is part of everybody's safeguarding responsibility. It is the duty of the School to ensure that members of the Lochinver House School community are protected from potential harm whilst they are on school premises.

The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks with using any form of communication which lies within the public domain. The digital world is an amazing place, vast and fast moving, but with few rules. It is therefore imperative that clear rules, procedures and guidelines are implemented to minimise risks whilst pupils use these technologies:

- Being vulnerable to inappropriate contact from strangers.
- Cyber-bullying, grooming, exploitation, image-based abuse, misinformation and harmful online content.
- Online content which is abusive, offensive, or pornographic.
- The use of social media to encourage extremism.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices.
- Exposure to misinformation and disinformation, including false or misleading content that can distort pupils' understanding of current events, health, or social issues.
- Engagement with conspiracy theories and other forms of online manipulation that may influence beliefs or behaviours in harmful ways.
- Harmful online conduct, such as peer pressure to participate in risky challenges, oversharing personal information, or engaging in trolling or harassment.
- Risks associated with online commerce, including scams, exploitation through in-game purchases, and exposure to advertising that targets children inappropriately
- Issues with spam and other inappropriate email.
- Viruses.
- Deepfakes and nudification 'de-clothing' apps recognised risks.
- Staff being aware of exposure to extreme sexual or physical violence online.
- AI-generated images, deepfakes, nudification apps and inappropriate use of generative AI.
- Recognition that pupils may try to bypass school filtering (using VPNs, etc.).
- Children may be victims of AI-enabled bullying, harassment, humiliation, coercion or exploitation.
- Sharing nudes and semi-nudes.

Whilst the School endeavours to safeguard and mitigate against all risks, we will never be able to completely eliminate them all. Any incidents that may come to our notice will be dealt with quickly and according to the School's policies.

The involvement of pupils and parents is vital to the successful use of digital technologies. This policy aims to inform how parents and pupils are part of the procedures and how pupils are educated to be safe and responsible users so that they can make good judgments about information they see, find and use. The School will continue to provide Online Safety information for parents, through the website, in newsletters and at events. The support of the parent body is key so they understand their role in supporting their children to behave appropriately and keep themselves safe online.

Aims of this Policy

- To ensure the safeguarding of all pupils within the school by detailing appropriate and acceptable use of online and digital technologies.
- To outline the roles and responsibilities of all pupils, staff and parents.
- To ensure all pupils, staff and parents are clear about procedures for misuse of any online technologies.
- To develop links with parents and the wider community to ensure continued awareness of online technologies.
- To clearly explain rules if authorised to access the School Wi-Fi. Parents and visitors to the School are prohibited to access the school Wi-Fi. Parents and visitors are prohibited from using mobile devices including smart

glasses, whilst on the School premises. If staff would like to use the Wifi on their personal device they should take this device to IT who will enter the code for them.

Curriculum and Tools for Learning

Online Safety is embedded within our curriculum. The School provides a comprehensive curriculum for Online Safety which enables pupils to become informed, safe and responsible, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through computing and/or PSHE lessons. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. 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.

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

The following concepts, skills and competencies are taught through the school in an age-appropriate manner:

- Digital citizenship.
- Future work skills.
- Internet literacy.
- Making good judgments about websites and emails received.
- Knowledge of risks such as viruses, and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File-sharing and downloading illegal content.
- The impact and use of Artificial Intelligence
- Uploading information – knowing what is safe to upload, and not to upload personal information.
- Where to go for advice and how to report abuse.

Early Years Use of Mobile Phones or Device - Statutory Regulation

The Early Years Safeguarding and Welfare Requirements (para 3.5) require all schools to have a clear policy on the use of mobile phones, cameras and other electronic devices with imaging and sharing capabilities. Lochinver House School does not permit the use of **personal** mobile phones and cameras, or other electronic devices with imaging and sharing capabilities by staff where children are present.

Email

Adults issued with a School email account must use this for all official communication. Under no circumstances should staff contact pupils, parents or conduct any School business using a personal email address. Employee email accounts are retained indefinitely.

Pupils may only use School approved accounts on the School system and only for educational purposes. Pupil email accounts are deleted when they are no longer a pupil of the School.

Emails created or received as part of any School role will be subject to disclosure in response to a request for information under the Data Protection Act 2018. All staff are expected to use email professionally and responsibly.

Filtering and Monitoring Safeguarding Measures

The School's Designated Safeguarding Lead (DSL) has lead responsibility for online safety, including understanding the filtering and monitoring systems and processes, in place at the School.

The School's internet has a robust filtering system which is set at an age-appropriate level such that inappropriate content is filtered. This filtering system is reviewed termly to ensure filters remain effective. The system logs all attempts to access the internet, including all attempts to access inappropriate content.

Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and iPads, and is updated on a regular basis. Security measures are in place to ensure information about our pupils cannot be accessed by unauthorised users. Strong encryption is used on the wireless network to provide good

security.

Incident Reporting
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. If this situation occurs the pupil or adult must report the incident immediately to the DSL/DDSL team using CPOMS and the School's Online Safety Incident Reporting Form (Appendix 2).
Where such an incident may lead to significant harm, safeguarding procedures should be followed. The School takes the reporting of such incidents seriously and where judged necessary, the DSL/DDSL team will refer details to Children's Social Care or the police.

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.

Monitoring
Appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. The School will monitor the use of online technologies and the use of the internet by pupils and staff. Classroom and computing teachers will conduct regular audits with pupils to assess their knowledge and understanding of issues related to Online Safety and act on any areas of vulnerability.

To audit digital safety and the effectiveness of this policy, the following questions should be considered:
- Has recording of Online Safety incidents been effective – are records kept?
- Did the School feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the School's ability?
- Do all pupils demonstrate an awareness of online appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use in the School?
- Do all members of the School community know how to report a problem?
- Is Online Safety observed in teaching and present in curriculum planning documents?

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 Lead with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils and families.

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)
- adult material that breaches the Obscene Publications Act in the UK
- promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- 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

- any material that may bring the School or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not:

- Reveal or publicise confidential or proprietary information.
- Interfere intentionally with the normal operation of the internet connection, including the propagation of computer viruses.
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the School.
- Use the School's hardware and Wi-Fi facilities for running a private business.
- Intimidate, threaten or cause harm to others.
- Access or interfere in any way with other users' accounts.
- Use software or hardware that has been prohibited by the School.

School devices should be used to conduct School business outside of School. Where this is not possible and a personal device needs to be used, a closed monitored system (e.g. Remote Desktop) must be set up by the school on said personal device. Cloud services can also be used eg Office365 but staff members must ensure that they sign out after use and that passwords are not saved. School data must not be stored on devices not belonging to the School. Staff members must ensure that they regularly check for viruses and keep all software up to date on any personal device they are conducting school business on.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

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 a member of Lochinver House School's Senior Leadership Team (SLT).

Parents and Visitors

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. It is important that parents understand the crucial role they play in this process. The School seeks to regularly consult and discuss Online Safety with parents 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 a variety of sources including the weekly bulletin.

All parents have access to a copy of this policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

As part of the approach to developing Online Safety awareness with pupils, the School may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites.

The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

Parents should be aware that the School cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils, and the possibility of pupils accessing inappropriate content. However, should parents or guardians become aware of an issue, we strongly encourage prompt communication with the school so we can offer advice and support. The school has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

At the start of every academic year (or when a new pupil joins), the School issues the Pupil – Parent iPad User Agreement which parents will be asked to read, discuss and co-sign with their children. Agreements are issued

when pupils are first given a School iPad in Year 5 or to new joiners in Year 6, 7 or 8. For information this can be found Appendix 5.

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 during lessons, duties or other formal School time. They should be switched off or silent at these times. Under no circumstance does the School allow a member of staff to contact a pupil or parent/carer using their personal device.

For staff including temporary and peripatetic, and visitors the 'Use of Mobile Devices in the EYFS' must be adhered to.

From Year 6 pupils are allowed to bring in personal mobile devices/phones into School with parental permission if they are required to go home independently. Parents are required to complete a Mobile Telephone Agreement which can be found Appendix 7 or requested from the School Office. Once the agreement has been signed and returned to the School, pupils are able to bring in their personal device. These devices must be handed in for safe keeping at the start of the day to the School Office.
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 or any member of staff.

Personally-owned mobile phones, mobile devices or cameras brought in to the School are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally-owned mobile phones, mobile devices or cameras. Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device.

Pupils

- Are involved in the review of Online Safety through discussion in lessons and other forums, in an age appropriate way.
- Are responsible for following the Online Safety Agreement whilst within school as agreed each academic year or whenever a new pupil starts at the school for the first time, and are required to sign that they have read and understood the rules.
- Are taught to use the internet in a safe and responsible manner through, for example, Computing and Digital Learning and PSHE lessons.
- Are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know.
- Are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues.
- Are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites.
- Are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free.
- Are taught to understand what is meant by Online Safety through age-appropriate delivery.
- Are taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies.
- Are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk.
- Are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by this policy.
- Must not circumvent internet access by using a personal device's cellular data services.
- Are taught that exposure to misinformation and disinformation, including false or misleading content that can distort their understanding of current events, health, or social issues.
- Are taught that engagement with conspiracy theories and other forms of online manipulation that may influence beliefs or behaviours in harmful ways.
- Are taught about harmful online conduct, such as peer pressure to participate in risky challenges, oversharing personal information, or engaging in trolling or harassment.

- Are taught about the risks associated with online commerce, including scams, exploitation through in-game purchases, and exposure to advertising that targets children inappropriately
- Are taught about (AI), how to evaluate AI-generated content critically, and recognise both the opportunities and risks associated with AI in the digital world.

Should a pupil be found to deliberately misuse digital or online facilities whilst at School, appropriate sanctions will be applied. If a pupil accidentally accesses inappropriate materials, the pupil is expected to report this to an appropriate member of staff immediately and take action to minimise the screen or close the window. Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment. Should a pupil use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our Behaviour Policy. Please see Appendix 1.

Social Media

When used correctly, parents can use a School's social media site as a source of reliable information. Social Media, however, should not be used to discuss School issues, either positive or negative as this could bring the School into disrepute and affect families and children. Parents should 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:

- The School will collect the facts as soon as they are aware of adverse comments relating to the School. The School will not become engaged in responding directly.
- If the allegations made against a member of staff or a pupil are of a serious nature, these will be formally investigated. This may involve the police.
- If there is a risk of serious damage to the School's reputation or the reputation of individual members of staff, professional legal advice will be sought.
- The School will contact the complainants and invite them to a meeting to resolve the situation.

Staff

The following responsibilities are for **all** adults within the school:

- Adhere to the Staff Code of Conduct including Acceptable Use Policy.
- Implement the pupil E Safety Agreement.
- Be up to date with digital knowledge appropriate for different age groups.
- Be vigilant when using technology as part of lessons.
- Model safe and responsible use of technology.
- Provide reminders and guidance to pupils on Online Safety.
- Ensure that pupils are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner.
- Not leave a computer or other device unattended whilst they are logged on.
- Lock away or safely secure all portable ICT equipment when not in use.
- Not connect with any pupil under the age of 18 on any social networking site, or via personal mobile phones and follow the school's Social Guidelines.
- Protect confidentiality and not disclose information from the network, or pass on security passwords.
- Ensure any information subject to data protection legislation, namely, the General Data Protection Act 2018 (as amended, extended or re-enacted from time to time), is not stored on unencrypted portable media or transported in an unsecure form.
- Use discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute.
- Not make or take personal calls or engage in personal texting when they are on duty.
- Report any concerns about a pupil related to safeguarding and Online Safety to the Designated Safeguarding Lead.
- Report accidental access to inappropriate materials to the Designated Safeguarding Lead so that inappropriate sites are added to the restricted list.
- Only use school owned devices and memory cards to take photographs or videos.

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school,

a report must be made to the Head immediately. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary. Please see Appendix 1.

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 Data Protection Act 2018 they are used only with the written consent of parents 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 at any time.

Photographs and images of pupils are stored on the School's agreed secure networks and devices which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by the Senior Leadership Team.

Video and Photography at School Events

Parents or visitors are not permitted to have visible any mobile storage device including mobile phones whilst on School premises and they must never be used around pupils regardless of age.

For events on the school premises such as class assemblies and nativity performances, parents may be given specific permission to take photographs or videos of their children but strictly on the agreement this is for private use only and never for publication or use on social media; this includes any uploading to WhatsApp, including groups set up by class and year representatives.

Visitors and Visiting Speakers

- Will not use their personal mobile devices and other devices with camera functions, imaging and sharing capabilities whilst on School premises. Such devices must be switched off and out of sight. Any exception must be pre-arranged.
- Where appropriate and working with EYFS children will adhere to the 'Use of Mobile Devices in the EYFS' policy.
- 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.
- Will not give out their personal details such as mobile phone number, email address, and social media account details to pupils and parent/carers. Where appropriate the School may share their professional contact details with parents/carers provided they have given authorisation.
- Understand their visit to the School may give them access to privileged information about pupils, staff, School systems and plans. Such information should never be shared online, including on social media sites.
- Will pre-check for appropriateness all internet sites intended for use whilst in School including checking the acceptability of other material visible on the site. They will not free-surf the internet in front of pupils and, if in any doubt about the appropriateness of the content, will check with their contact in the School.

The School's Responsibilities

The School takes its responsibilities in relation to the acceptable use of technology by pupils and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly. The Designated Safeguarding Lead (DSL), Head and governors have ultimate responsibility to ensure that appropriate online safety provisions are in place and online safety practice is embedded and monitored.

This policy is reviewed, authorised and approved by the Board of Governors and updated as needed on an interim basis by the Safeguarding team.

Reviewed By	Head of Computing & DSL
Approval Body/ Committee	Education
Last Review	Autumn 2026
Next Review	Autumn 2027
Policy Linked To	Acceptable Use Policy, AI Policy, Anti-Bullying Strategy, Behaviour Policy, Child Protection and Safeguarding Policy (incorporating Staff Behaviour and Code of Conduct), Data Protection Policy, Health and Safety Policy, Privacy Notice, Personal, Social, Health and Education (PSHE) Policy, Remote Learning Policy, Spiritual, Moral and Cultural (SMSC) Policy, Use of Mobile Devices in the EYFS Policy

Any data held in relation to the content of this policy will be managed in accordance with our Data Protection Policy and Privacy Notice.

Appendix 1 - Procedures in the Event of a Breach of this Policy

An inappropriate website is accessed inadvertently:

- Report to Designated Safeguarding Leader who will record this in a The Safeguarding Log.
- The Designated Safeguarding Leader will contact IT Support via email so that it can be added to the barred or restricted list.

An inappropriate website is accessed deliberately, or ICT equipment used inappropriately:

- Ensure that no one else can access the material, by shutting down the computer.
- Record the incident in writing.
- Report to the Head immediately.
- The Head applies the Behaviour Policy.

A pupil uses the Internet whilst not on school premises in such a way to cause hurt or harm to a member of the school community

- Record the incident in writing
- Report to Head of Pastoral immediately
- Behaviour policy applied

An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Designated Safeguarding Leader immediately.
- Ensure the device is shut down and record the nature of the material.

An adult has communicated with a pupil, or used ICT equipment, inappropriately:

- Ensure the pupil is reassured.
- Report to the Head who should follow the Child Protection and Safeguarding Policy and Procedure (if relevant).
- Preserve the information received by the pupil if possible, and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate use is established, contact the Head. If the allegation is made against the Head inform the Chair of Governors immediately, and follow the Child Protection and Safeguarding Policy and Procedure.

Threatening or malicious comments are posted to the school website or distributed via the school email system (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the Head immediately and follow the Child Protection and Safeguarding Policy and procedure as necessary.

Images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere:

- The Head must be informed.

Appendix 2 – Incident Reporting Form

Any member of the school community can raise a concern about an Online Safety incident. If you have witnessed or experienced an incident, please record the incident on CPOMS, also complete the form, providing as much detail as possible, and return to the Designated Safeguarding Lead.

NAME of person reporting the incident:			
Signature and date:			
Where did the incident take place?			
Date and time of incident?			
Who was involved in the incident?	Staff members names:		
	Parents/carers names?		
	Pupil/young persons names?		
	Other (please specify)		
Type of Incident – indicate as many as apply		Accessing age inappropriate websites, apps and social media	
		Accessing and/or sharing terrorist material	
		Accessing someone else's account without permission	
		Accessing, sharing or creating pornographic images and media	
		Accessing, sharing or creating violent images and media	
		Breaching copyright regulations	
		Creating an account in someone else's name to bring them into disrepute	
		Deliberately bypassing security	
		Drug/bomb making material	
		Forwarding/spreading chain messages or threatening material	
		Grooming	
		Hacking or spreading viruses	
		Online bullying or harassment (cyber bullying)	
		Online gambling	
		Posting images without permission of all involved	
		Posting material that will bring an individual or the school into disrepute	
		Racist, sexist, homophobic, religious or other hate material	
		Sexting/Child abuse images	
		Other breach of acceptable use agreement, please specify:	
Full description of the incident:	Include what, when, where, how?		
Name of all social media involved?	Specify Twitter, FaceBook, Whatsapp, snapchat, Instagram, etc		
Evidence of the incident	Specify any evidence available but do not attach		

Appendix 3 – Online Safety Agreement for Pupils in Early Years and Year 1

The internet and mobile technologies have become integral in learning. We expect all pupils to be safe and responsible. Please read and discuss these computing and Online Safety rules with your child and return this document when signed by you both. If you have any concerns or would like some explanation, please contact your child's class teacher.

All children must follow these rules. The teachers at Lochinver House School will show pupils how to use the School iPads and other mobile technologies.

This is how I stay safe:

- I will use iPads and other mobile technology safely and carefully.
- I will only use the iPads and other mobile technology when a grown up is nearby.
- I will only use activities allowed by a teacher or teaching assistant.
- I will always ask if I need help or if I am worried I may have done something wrong.
- If I see something that upsets me, I will tell my teacher or another adult.
- I will never give my name or address to people I do not know.
- I will take care of all the equipment.

I know that if I do not follow the rules:

I may not be able to use the iPads or other mobile technology.

I understand the rules and have talked to my parents about what they mean.

Pupil's Name / Signature:		**Class:**	

I have discussed the Online Safety rules with my child and support this code at Lochinver House School.

Parent's signature:		**Date:**	

Appendix 4 – Online Safety Agreement for Pupils in Years 2 – 4

Using the internet is a privilege; therefore, we need to make responsible choices while using the internet. We agree that we should all be able to feel safe and that the consequences of not practising safe and responsible usage of the internet can be serious and dangerous.

My behaviour when using the iPad, laptops and the Internet at school

- I move around the classroom safely when working an iPad.
- I use two hands when I hold an iPad.
- I never change the settings or background of the school iPads.
- I will not share my name, address, password, phone number, photographs or plans online.

I will not bring in mobile phones or devices, iPads, smart watches or smart glasses into school.

- I will ask for permission before taking and sharing photographs of others.

Finding Information and Research on the Internet

- I understand that at school only websites approved by teacher can be used and out of school only websites that are approved by my parents and family.
- I understand that at school, use of the Internet is only allowed with staff permission and supervision.
- I understand that outside school, parental permission and supervision is needed for use of the Internet.
- I understand that I should not believe everything I read – I should always double-check my facts.
- I respect copyright and never copy and paste text from the Internet.
- I can use images from the Internet to enhance my work.
- I should always select pictures appropriate to the topic.

Sending and receiving messages

- I am respectful when sending messages; we talk to each other online the way we would talk to each other in person.
- I take care to talk online only to people I know.

<u>If we see anything that makes us feel uncomfortable, we do not like or we are not sure about, we tell an adult straight away! Stop and Show!</u>

I have read this guide with my parents and I agree to follow Online Safety rules at all times.

Pupil's Name/Signature:		**Class:**	

I confirm I have discussed the Online Safety rules with my child and support this code at Lochinver House School.

Parent's signature:		**Date:**	

Appendix 5 – Online Safety Agreement for Pupils in Years 5 – 8

My Online Safety rules:

• I will only use school IT equipment and online services for activities approved by school staff and will take care not to damage any devices, including keeping magnetic sources away to prevent potential issues.

• I am responsible for my account and passwords. I will not share my passwords with anyone except my parents/carers and IT Support, and I will never use another person's account or password.

• I will use my school email address and credentials only for school work and will only sign up for online services or use AI tools when approved by my teacher and, where required, my parent/carer. If I use AI to support my work, I will clearly state this.

• I will only bring approved devices to school. Watches must not have internet access or photo/video capabilities. I will seek permission before bringing a device to school or connecting any personal device to school equipment. I understand that smart glasses are not allowed in school.

• I will only open email attachments from trusted and approved sources. Any suspicious emails, attachments or online activity will be reported immediately to a member of staff or IT Support.

• I will communicate online in a polite, respectful and responsible manner and will always act respectfully towards the school and wider school community.

• If I see, receive or experience anything upsetting, inappropriate, unkind or unsafe online, I will not respond and will tell a teacher, parent/carer or another trusted adult immediately. I will also report concerns about cyberbullying.

• I will protect my own and others' personal information and privacy. I will not share personal details online and will only share images or videos of myself or others with the appropriate permission.

• I understand that people online may not always be who they claim to be. I will never arrange to meet someone I only know online and will report any such request immediately.

• Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this.

• I will respect copyright and intellectual property and will not copy or use the work of others and claim it as my own.

• I will ensure that anything I create, upload or share is appropriate, respectful and unlikely to cause harm or upset now or in the future.

•I understand that my actions online can be traced, both now and in the future, so I will make positive choices that help me build and maintain a good online reputation.

•I should assume that messages and content posted online cannot be deleted and must therefore use the 'stop and think' approach before doing so.

• I will use only age-appropriate games, apps and social networks and will seek advice from school staff whenever I am unsure whether something is acceptable.

• I understand that these rules are designed to keep me safe and that failure to follow them may result in appropriate action being taken by the school.

I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil's Name/Signature: _____ Date: _____

Parent(s)/Carer(s) name(s):_____ Date: _____

Parent(s)/Carer(s) signature_____ Date: _____

Appendix 6 – Pupil-Parent iPad Use Agreement

- All iPads remain the property of Lochinver House School.
- You will comply at all times with the School's Online Safety Policy. Failure to comply will mean you forfeit your right to participate in the iPad scheme and your iPad will be recalled.
- Your right to use and possess the iPad terminates no later than the last day of attendance at the School.
- I will not intentionally cause damage or harm to my School iPad, including keeping magnetic sources away to prevent potential issues.
- The vast majority of updates will be deployed to the iPads remotely; however, the School may occasionally recall the iPads to install essential updates. You must hand in your iPad for this purpose when requested.
- The School makes every effort to block inappropriate websites and content both inside and outside of School by installing a filtered browser on each device. Using software utilities or other means to access blocked content is a direct breach of the School's Acceptable User Policy.
- Limited personal use is permitted as long as it does not violate this agreement, the School's Online Safety Policy and Acceptable Use Policy.
- Inappropriate content will not be allowed on iPads and the presence of such materials will result in appropriate sanctions.
- Sound will be muted at all times unless permission is obtained from the teacher.
- iPads will have security applications installed. Deletion of security-related apps is prohibited.
- When your iPad is returned, you will lose all downloaded content unless it has been stored on iCloud. It is your responsibility to ensure that personal content is saved to a personal device before returning the iPad.
- The iPad comes equipped with a microphone, front and rear-facing camera, and video capability. Lochinver House School retains the rights concerning any image or recording and/or publishing of any pupil's work.
- You must obtain permission from a teacher before recording or photographing an individual, group or teacher or publishing a photograph of any School-related activity. Unauthorised images and recordings are subject to a school based sanction in accordance with the School's Behaviour Policy.
- In lesson time you must only use your iPad with the permission of your teacher.
- You must not use your iPad around the School site unless you have direct permission from your teacher.
- Your iPad should be protected with a suitably complex passcode at all times. This passcode should be known only by you/parents/IT Support to ensure the iPad is only used by you. Lochinver House School retains the right to bypass the security code.
- You may not lend your iPad to another pupil or borrow another pupil's iPad. Access to another person's account or iPad without consent or knowledge is considered hacking and is prohibited.
- Your iPad should not be modified in any way that will permanently alter it, either physically and/or electronically, other than instructed by a member of staff.
- You may not apply any additional stickers, marks or other decorations to the iPad supplied to you.
- You should not remove the iPad's case.
- You are responsible for bringing your iPad to School fully charged each day.
- You will follow all the rules as set out on the home screen of your iPad.

You will be liable for any replacement or repair costs. These will be added to your invoice. Your son may forfeit his right to retain use of a School iPad if he repeatedly damages his device or does not follow the agreements set out here. Items not covered by the School include damage of the iPad, cables, case, or power adapter, cosmetic damage, effects of normal wear and tear, third party products or effects that may damage the iPad, recovery of software or data and damaged/lost covers.

Pupil's Name/Signature: _____ Date: _____

Parent agreement

I have read and understood the School's Online Safety Policy and Pupil- Parent iPad Use Agreement, and discussed with my child.I agree to pay for any repair or replacement costs. I have discussed the Online Safety rules with my child and support this code at Lochinver House School.

Parent's signature: _____ Date: _____

Appendix 7 – Mobile Phone and Personal Device Agreement – Pupils

As a general rule, mobile phones and smart watches that offer connectivity should not be brought into School. They are not to be used during the School day and students are not allowed to carry them around the School site.

We do recognise that on occasion it may be necessary for pupils to have their phones, either on their journey to School, or for their time after the end of the School day. When this is necessary, on arriving at School, pupils must take their phone or device to the School office where there are lockers for their phones. Pupils will be responsible for the key to the locker they are using during the day. If a key is lost a charge will be made to replace it.

Any pupil found in possession of or using their phone during the day, without express permission, will have their phone confiscated and returned at the end of the School day.

Smart phones and other connected devices give pupils easy access to internet sites that the School would ordinarily guard against or prohibit with a fire wall. Parents should be aware of the potential for 'cyberbullying' stemming from handheld devices and you are advised to actively check your child's phone on a regular basis and to ensure that they are fully aware of the implications of using it in inappropriately.

Expected Conduct

- Pupils should only bring mobile telephones and/or smart devices to School when necessary, for example when travelling to School independently or going home with another pupil.
- Parental consent is required when pupils bring mobile telephones and/or smart devices to School, by signing the attached letter.
- Mobile telephones and/or smart devices must be stored in the lockers located in the School Office when pupils arrive at School and only collected when they make their way home.
- There may be exceptional circumstances when it is necessary for a pupil to contact parents or carers, and this must be done through the School office.
- There may be exceptional circumstances where a mobile telephone or smart device is needed to operate a medical device. This can only happen with the permission of the Deputy Head Pastoral.
- Mobile telephones and/or smart devices brought into School are the responsibility of the device owner. The School accepts no responsibility for their loss, theft or damage.
- The Acceptable Use Policy applies to all pupil personal devices.
- If a pupil breaches the expected conduct their mobile telephone and/or smart device will be confiscated and will be held by the Deputy Head Pastoral. The telephone or smart device will be released to a parent or carer at the end of the School day.
- Under no circumstances must mobile telephones and/or smart devices be used by pupils on the School site or School minibuses.

Trips from School

Mobile devices (including telephones) are not to be taken on trips away from the School site.

Incident Management

Any pupil who knowingly commits an offence will be accountable for their actions in line with the School's Behaviour Management and Exclusions Policy. Offences include, but are not limited to:

- cyberbullying
- accessing or sending inappropriate material or messages
- sending emails to large groups of users (spamming).

==========

Please return this signed slip to the School Office when your child next brings their device to School.

I consent to my child _____carrying their personal device to and from School and leaving it in the lockers provided during the School day.

Signed _____Parent/Guardian Date _____