Amble Links First School
Policy for Online Safety

Date Written:	**November 2023**
By:	**Paul Heeley**
Adopted by Governors:	
Date for Review:	

Online Safety Co-ordinator	Paul Heeley
Designated Safeguarding Lead/Deputy	Paul Heeley/Louise Cuthbertson
Designated Governor for Safeguarding	Mark Phillips
Data Protection Officer	Wallis Bath
Network Manager	John Harwood (Harwood Technical Solutions) harwoodts@gmail.com
Should serious online safety incidents take place, the following external persons/agencies should be contacted.	Richard Taylor (Online Safety Consultant) richard.taylor@northumberland.gov.uk Northumberland Local Authority Designated Officer – LADO lado@northumberland.gcsx.gov.uk

Introduction

At Amble Links First School we believe that Information Communications Technology (ICT) is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

This policy ensures that the school meets and exceeds the requirements for online safety set out in 'Keeping Children Safe in Education' (Sept 2023 paras 135-148) and should be read in conjunction with other policies including Behaviour Management, Mobile Phones and Anti-Bullying.

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to date technologies around school. ICT is a life skill and should not be taught in isolation.

ICT covers a wide range of resources including web-based and mobile learning. It is important to recognise the constant and fast paced evolution of ICT within our society as a whole. Internet technologies that children may be using in school and/or out of school include:

- Websites
- Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Video Broadcasting
- Music Downloading
- Gaming
- Smart phones
- Podcasting

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Amble Links First School, it is the responsibility of all staff to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.:

The 4 key categories of risk

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

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

This Online Safety Policy aims to ensure that exposure to risks are limited but that children are equipped with the skills and knowledge they need to use technology safely and responsibly and manage risks themselves

Whole School Approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school online safety procedures.

The Computing/Online Safety Lead (Paul Heeley – Headteacher) will ensure they are up to date with current guidance and issues through organisations such as Northumberland LA, CEOP (Child Exploitation and Online Protection), SWGFL advice and Childnet. They then ensure that staff and Governors are updated as necessary.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website and Facebook page
- procedures in the event of misuse of technology by any member of the school community
- their role in providing online safety education for pupils.

Staff are updated about online safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction as well as online safety training. School staff sign an Acceptable Use Policy (AUP) annually. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 5 for staff acceptable use agreement).

Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. It is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety.

- We provide opportunities within the Computing and PSHE curriculum areas to teach about online safety.
- Educating pupils on the dangers of technologies that may be encountered outside school also takes place when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the Computing curriculum.
- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are provided with online tools that allow them to report any concerns or worries that they may have

- Pupils are taught to critically evaluate materials and learn good searching skills through the Computing lessons and through the wider curriculum.
- Pupils are taught about the risks inherent in using online services through the 4 C's (Conduct, Content, Contact and Commerce)

Managing Internet Access
Children will have supervised access to Internet resources

- Staff should preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links. Google SafeSearch is enabled on all pupil accounts.
- If Internet research is set for homework, specific sites may be suggested. These should be checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents should be advised to supervise any further research.
- Our internet access is controlled through the Fortigate web **FILTERING** service (details at: https://bit.ly/2LhLIvC) - **MONITORING** of access is provided through KBR Networking Solutions and access reports can be provided where necessary. A captive portal ensures that activity on all devices in school can be monitored. Weekly report of filtering and monitoring are checked by the Headteacher and any concerns are recorded on the CPOMS (pupils) or Confide (Staff systems).
- Staff and pupils are aware that school based email and internet activity is monitored and explored further if required.
- Monitoring – All school computers are monitored through Senso Cloud, purchased through Northumberland County Council. This is monitored in school and by the local authority.
- School based email is provided to pupils through School360 using Google Mail – pupils are only able to send and receive emails within the secure School360 domain.
- If pupils discover an unsuitable site the incident is reported immediately to a member of staff –this will be logged as an online safety incident using the CPOMS system and referred to the Online Safety Co-ordinator.
- If staff members discover an unsuitable site the incident is reported immediately to the Headteacher – this will be logged as an online safety incident using the Confide system.
- It is the responsibility of the school, by delegation to the network manager (John Harwood), to ensure that antivirus protection is installed and kept up-to-date on all school machines.

E-mail
The use of email within school is an essential means of communication for staff. Email should not be considered private. Educationally, email can offer significant benefits although recognise that pupils need to understand how to style an email in relation to their age.

- Pupils are introduced to email as part of the Computing Curriculum. School based email is provided to pupils through School360 using Google Mail – pupils are only able to send and receive emails within the secure School360 domain.
- The school gives staff their own School360 email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils must immediately tell a member of staff if they receive an offensive e-mail – this should then be referred to the Online Safety Co-ordinator.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform the Online Safety Co-ordinator/Headteacher if they receive an offensive e-mail.

Publishing pupil's images and work

On a child's entry to the school, and then annually, parents will be asked to give consent for their child's photo to be taken and to use their child's work/photos in the following ways:

- on the school website and Facebook page
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances such as in local or national newspapers.

Pupils' names will not be published alongside their images online.

Care will be taken to ensure that pupils are appropriately dressed and not participating in activities that might bring the school into disrepute.

Staff are allowed to take digital video/images to support the aims of the school. Wherever possible, images should be taken on school devices. Governors have carefully considered the relevant guidance, benefits, risks and budget implications of staff using personal devices to take photographs of pupils for school publications and social media. It has been agreed that the Headteacher may use their mobile phone to take and upload images of pupils to the school's website and social media page following the above guidance. Staff accompanying school visits may also use their personal devices to take photographs of pupils that support the aims of the visit. All photographs of pupils should be immediately deleted from personal devices as soon as they have been transferred to the school's Google Drive or uploaded to the school website or social media page.

In accordance with guidance from the Information Commissioner's Office, parents and relatives are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and protection these images should not be made publicly available on social networking sites.

Social Networking
We block/filter access for pupils to social networking sites. Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing Emerging Technologies
Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Mobile Phones
We have a separate policy for the use of mobile phones in school.

Data Protection
Amble Links First School complies with all relevant data protection legislation.

Our named Data Protection Officer is: Wallis Bath

Policies can be found at: http://www.amblelinks.northumberland.sch.uk/website/gdpr_-_data_protection/352900

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
-
- When personal data is stored on any portable computer system, memory stick or any other removable media:
- The data must be encrypted and password protected.

- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete
- It is strongly recommended that staff store all information on the school's cloud based storage system accessible through School360.

Responding to online safety incidents/complaints

The school will take all reasonable precautions to ensure that everyone is kept safe online. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to online safety should be made to the Online Safety Co-ordinator. Any complaint about staff misuse must be referred to the Head teacher.

- All online safety incidents will be logged using the school's CPOMs system(pupils) or Confide (Staff)
- The Online Safety Co-ordinator will investigate and respond appropriately and record these responses using the CPOMS system.
- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Parents of pupils involved will be informed of the incident and will be expected to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our online safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyberbullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Supporting the person being bullied

Support shall be given in line with the Anti-Bullying Policy. This may include:

- Giving reassurance that the person has done the right thing by telling someone
- Informing parents
- Making sure the victim knows not to retaliate or return the message
- Helping the victim keep relevant evidence for any investigation (taking screen capture shots, not deleting messages)
- Checking that the victim knows how to prevent it from happening again e.g. blocking contacts, changing contact details
- Taking action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down.

Investigating Incidents

All bullying incidents should be recorded and investigated in the CPOMS incident log as any other bullying or online safety incident. We will then investigate as fully as any other bullying incident (refer to Anti-Bullying Policy)

Working in Partnership with Parents

Pupils and parents are expected to follow an age appropriate Acceptable Use Agreement. These are discussed with pupils annually.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section may be inappropriate in a school context and that users, or groups of users, as defined below, may not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated persons	Unacceptable	Unacceptable and Illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					**X**
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					**X**
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					**X**
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					**X**
Promoting radicalisation or extremism				**X**	**X**
Pornography				**X**	
Promotion of any kind of discrimination				**X**	
Threatening behaviour, including promotion of physical violence or mental harm				**X**	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				**X**	
Using school systems to run a private business				**X**	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				**X**	
Infringing copyright				**X**	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				**X**	
Creating or propagating computer viruses or other harmful files				**X**	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				**X**	

On-line gaming (educational)	**X**				
On-line gaming (non-educational)		**X**			
On-line gambling				**X**	
On-line shopping / commerce			**X**		
File sharing				**X**	
Use of social media			**X**		
Use of messaging apps			**X**		
Use of video broadcasting eg Youtube			**X**		

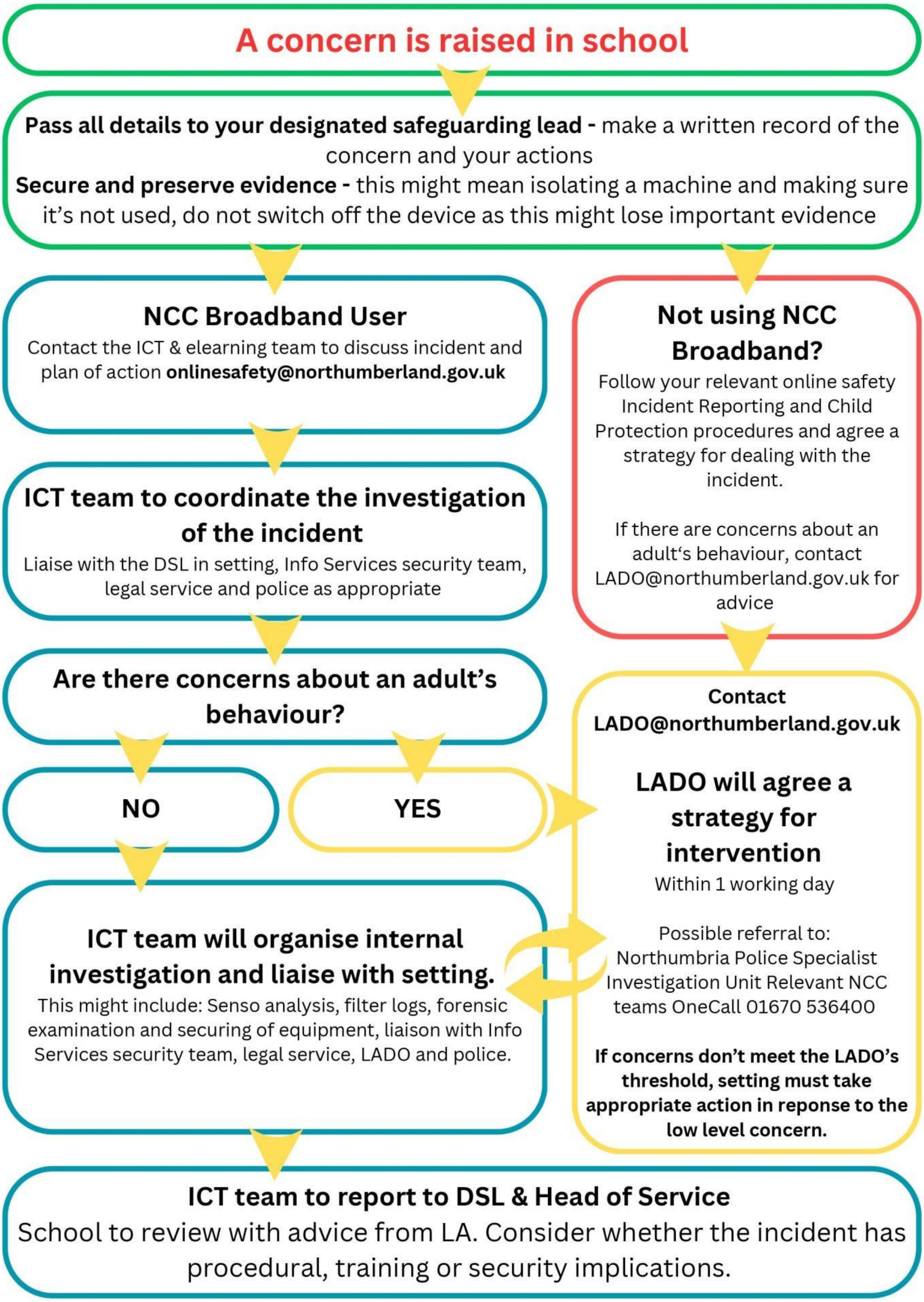
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above). SWGfL BOOST can be used to support dealing with serious incidents. This includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through how to respond, forms to complete and action to take when managing such incidents.

Serious Online Safety Incidents

The flowchart below details how serious online safety incidents of all types will be dealt with.

Reporting an online safety incident - all settings



A concern is raised in school

Pass all details to your designated safeguarding lead - make a written record of the concern and your actions

Secure and preserve evidence - this might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence

NCC Broadband User

Contact the ICT & elearning team to discuss incident and plan of action **onlinesafety@northumberland.gov.uk**

ICT team to coordinate the investigation of the incident

Liaise with the DSL in setting, Info Services security team, legal service and police as appropriate

Are there concerns about an adult's behaviour?

NO

YES

ICT team will organise internal investigation and liaise with setting.

This might include: Senso analysis, filter logs, forensic examination and securing of equipment, liaison with Info Services security team, legal service, LADO and police.

Not using NCC Broadband?

Follow your relevant online safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.

If there are concerns about an adult's behaviour, contact LADO@northumberland.gov.uk for advice

Contact LADO@northumberland.gov.uk

LADO will agree a strategy for intervention

Within 1 working day

Possible referral to:
Northumbria Police Specialist Investigation Unit Relevant NCC teams OneCall 01670 536400

If concerns don't meet the LADO's threshold, setting must take appropriate action in reponse to the low level concern.

ICT team to report to DSL & Head of Service

School to review with advice from LA. Consider whether the incident has procedural, training or security implications.

Where there are concerns that the promotion of radicalisation or extremism is taking place this should be reported immediately in line with the school's policies for Child Protection and 'Tackling Extremism and Radicalisation' policy that support the PREVENT agenda. Concerns should immediately reported to the Local Authority Designated Officer (LADO) – 01670 62397or to the police: preventmailbox@northumbria.pnn.police.uk.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. The tables in Appendix 1 and Appendix 2 identify likely procedures that would be followed in such cases.

Policy Review

This policy will be formally reviewed annually or sooner if necessary.

Appendix 1

Possible School Actions and Sanctions –Staff

Incidents:	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to technical support staff for action re filtering / security etc	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	X	X	X	X		X	X
Inappropriate personal use of the internet/social media/ personal email	X			X			
Unauthorised downloading or uploading of files	X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X				X		X
Deliberate actions to breach data protection or network security rules	X	X			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X
Involvement in the promotion of radicalisation or extremism	X	X	X	X	X	X	X
Using personal email/social networking /instant messaging/ text messaging to carrying out digital communications with pupils	X	X	X		X	X	X
Actions which could compromise the staff member's professional standing	X				X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X

Appendix 2

Possible School Actions and Sanctions –Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).		X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X							
Unauthorised use of mobile phone / digital camera / other mobile device		X						
Unauthorised use of social media / messaging apps / personal email	X							
Unauthorised downloading or uploading of files		X						
Allowing others to access school / academy network by sharing username and passwords		X		X		X		
Attempting to access or accessing the school / academy network, using another student's / pupil's account		X				X		
Attempting to access or accessing the school / academy network, using the account of a member of staff		X			X	X		
Corrupting or destroying the data of other users		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X	X
Involvement in the promotion of radicalisation or extremism		X	X	X	X	X	X	X

Appendix 3

Amble Links First School

Pupil ICT and Internet Acceptable Use Agreement (Early Years/KS1)

This is how we stay safe when we use computers:

- I will ask a grown up before I use the internet
- I will take care of computers and other equipment and use them properly
- I will not tell anyone my password or use someone else's password.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets or worries me on the screen.
- I will never do anything on the computer that could be unkind or upset someone.
- I will never communicate with strangers online

I understand that the school will monitor everything I do on the computer and I know that if I break the rules I might not be allowed to use a computer, even if it was done out of school.

Signed (child):…………………………………………

Signed (parent): ……………………………………….

Appendix 4

Amble Links First School

Pupil ICT and Internet Acceptable Use Agreement (KS2)

Our school provides Internet access to help our learning. To help keep myself and others safe when we use computers and the internet I agree that:

- I will only use the internet in school when I have permission and will take care of any ICT equipment that I use
- I will not tell others my password or use other people’s passwords
- I will make sure that all ICT contact with others is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. **If I come across anything like this I will tell my teacher immediately**
- I will not give out personal information online
- **I will immediately report any unpleasant messages sent to me** because this would help protect other pupils and myself.
- I understand that others may read or share messages I receive or send.
- I will not use the computer to communicate with stranger and I will never arrange to meet a stranger
- I will not bring a mobile phone to school
- I will only take a photograph or video of someone if they say it is alright
- I will never do anything on the computer that could be unkind or upset someone
- Anything I do online will be responsible, polite and sensible

I understand that the school will monitor everything I do on the computer and I know that if I break the rules I might not be allowed to use a computer, even if it was done out of school.

Signed (child):……………………………………………

Signed (parent): …………………………………………..

Appendix 5

AMBLE LINKS FIRST SCHOOL

INTERNET AND INFORMATION SYSTEMS ACCEPTABLE USE POLICY AND AGREEMENT FOR STAFF AND VOLUNTEERS

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be respectful and responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the safety and security of children, other users or systems at risk.
- That staff and volunteers will have good quality and appropriately filtered access to ICT and the internet to enhance their work, to enhance learning opportunities for and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users, especially our pupils. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the children in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I will ensure that I logout or lock any school computer that I am logged in to when leaving it unattended.
- All data that I store should be held on the secure Google Drive provided by the school through the School360 system. USB memory sticks should only be used if absolutely necessary – **only encrypted USB sticks may be used on school devices**.

understand that the school will monitor my use of the ICT systems, email and other digital communications using theFutures Cloud and Fortinet systems.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, School360 etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person. (Online Safety Co-ordinator/Designated Safeguarding Lead: Paul Heeley. Deputy Designated Safeguarding Lead: Louise Cuthbertson)
- I will only use my personal device to take photographs during school visits. I will delete any images taken as soon as possible after they are uploaded or transferred to school systems.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission. Where these images are published on the school website it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any online activity that may compromise my professional responsibilities or the school's staff code of conduct.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my own mobile devices (laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use included in the school's policy for Mobile Phones. I will ensure that any such devices are protected by up to date anti-virus software. **It is strongly recommended that staff switch Bluetooth off their mobile devices whilst on the school premises.**

- I will not use personal email addresses on the school ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will ensure that my data is regularly backed up.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act etc) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not install or attempt to install programmes of any type on a device, or store programmes on a device, nor will I try to alter device settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.

- I understand that the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened using the agreed school reporting system using the relevant document on Google Drive.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority or, in the event of illegal activities, the involvement of the police.

AMBLE LINKS FIRST SCHOOL

INTERNET AND INFORMATION SYSTEMS ACCEPTABLE USE POLICY AND AGREEMENT FOR STAFF AND VOLUNTEERS

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

FOR GUEST USERS ONLY:

Each guest user will be allocated a unique username and password by the Online Safety Co-ordinator or Network Manager.

By signing this agreement, you agree to the school internet and information systems acceptable use policy and agreement for staff and volunteers and understand that your network activity and internet use being tracked and monitored.

Guest Account Name

Name of User

Signed

Dates applicable