Amble Links Primary School

Digital Safety Policy

Date approved:	**November 2025**
Review date:	**November 2027**

Digital Safety Co-ordinator	Paul Heeley
Designated Safeguarding Lead/Deputy	Paul Heeley/Sarah Black
Designated Governor for Safeguarding	Mark Phillips
Data Protection Officer	Wallis Bath
ICT Manager	John Harwood (Harwood Technical Solutions) harwoodts@gmail.com
Should serious digital safety incidents take place, the following external persons/agencies should be contacted.	Jordan Graham (Online Safety Consultant) jordan.graham@northumberland.gov.uk Northumberland Local Authority Designated Officer –LADO lado@northumberland.gov.uk

SEE APPENDIX 6 FOR FLOWCHART FOR REPORTING AN ONLINE SAFETY INCIDENT

1. Aims

Our school aims to:

- Have robust processes in place to ensure the digital safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to digital safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also takes into consideration the expectations of the Online Safety Act (2023)

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Governing Board

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

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

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

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

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place

DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

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

The governor who oversees digital safety is **Mark Phillips.**

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that digital safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including digital safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead (DSL)

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

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy every 2 years (or sooner if necessary) and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any digital safety issues or incidents
- Managing all digital safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring

- Making sure that any digital safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on digital safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on digital safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including digital safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school.
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly. This includes a backup system as part of a disaster recovery plan.
- Ensuring that all devices are fully updated with security updates
- Supporting investigation of digital incidents if required

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting directly to Paul Heeley.
- Following the correct procedures by contacting Paul Heeley if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any digital safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Support the content of this policy
- Immediately report any concerns relating to digital safety

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about digital safety

Pupils will be taught about digital safety as part of the curriculum.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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

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

Pupils in **Key Stage 2** will be taught to:

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

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

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online

- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

At appropriate times older pupils will be made aware of the latest risks that they may face online and how to deal with these:

Synthetic Media: *(content created or modified using artificial intelligence (AI). As an emerging form of media, it has also been referred to as "AI-generated media," "media produced by generative AI," and sometimes "personalised media" or "personalised content." In mainstream media, synthetic content (and synthetic sexual content) is often referred to as a "deepfake" when it involves the realistic manipulation of video or audio to alter a person's likeness or voice)*

Misinformation *(false or misleading information that is shared by someone who believes it to be true. They are not intending to cause harm but by passing the information on they can mislead others)*

Disinformation (including fake news) (*this is where information is deliberately created and spread to cause harm, mislead or manipulate people*)

Conspiracy Theories (*stories or ideas that claim events are secretly controlled by powerful groups, often without evidence),*

Cyberflashing *(sending of unsolicited sexual images intended to alarm or distress)*

Epilepsy Trolling *(Sending of flashing images aiming to trigger seizures or cause distress*

Threatening Communications *(sending threats of serious harm, death or violence)*

Encouraging serious self-harm *(Promoting or encouraging serious self-harm online, even if harm does not occur)*

Sharing of Intimate Images (including deepfakes) *(Sharing or threatening to share sexual images without consent, including AI generated content)*

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

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

5. Educating parents/carers about digital safety

The school will raise parents/carers' awareness of digital safety in letters or other communications home, and in information via our website and/or Facebook page. This policy will also be shared with parents/carers.

Curriculum planning, including the teaching of digital safety will be shared on the school website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Cyberbullying is addressed through PSHE lessons, Computing/digital safety lessons and through whole school/class assemblies. It is also addressed with specific groups of children where necessary.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher/Deputy Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Our school Behaviour Policy (containing details of searching and confiscation)

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)/ Synthetic Media

Further information on Synthetic Media can be found HERE.

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Amble Links Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Amble Links Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and behaviour policies. Specific guidance and support on responding to incidents involving synthetic media can be found HERE.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7.Managing Internet Access

7.1 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://drive.google.com/file/d/1yZD4YtXcO-kJhZMclHGN6PainvTpbM8V/view) - Monitoring of access and filter activation is provided through KBR Networking Solutions. Daily safeguarding reports are provided and checked by the headteacher. A captive portal ensures that activity on all devices in school can be monitored. Any concerns are recorded on the CPOMS (pupils) or Confide (Staff systems).
- MONITORING – All school computers are monitored through Senso Cloud, purchased through Northumberland County Council. This is monitored in school and by the local authority. (Details at: https://drive.google.com/file/d/1MmtQtU_rjWgPoTmrXLjUkTC8-iTxl8Ac/view)
- Staff and pupils are aware that school-based email and internet activity is monitored and explored further if required.
- 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 digital safety incident using the CPOMS system and referred to the Digital Safety Co-ordinator.
- If staff members discover an unsuitable site the incident is reported immediately to the Headteacher –this will be logged as a digital safety incident following our policy for low level concerns.
- It is the responsibility of the school, by delegation to the ICT manager (John Harwood), to ensure that antivirus protection is installed and kept up-to-date on all school machines.

7.2 Email

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 Digital 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 Digital Safety Co-ordinator/Headteacher if they receive an offensive e-mail.

7.3 Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

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

8. Publishing pupils' images and work

On a child's entry to the school, and then annually through the Arbor app, 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.

9. Pupils bringing mobile devices to school

Children in Years 4,5 & 6 may bring mobile devices into school. There is an expectation that these devices are kept in a bag or pocket when within the school grounds and then switched off and handed to a member of staff for safe keeping during the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

We have a separate policy for Mobile Phones.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected using appropriately strong passwords
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from John Harwood (ICT Manager)

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, anti-bullying and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. See appendix 4

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. See appendix 5.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

12.1 Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and digital safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include digital safety, at least every 2 years. They will also update their knowledge and skills on the subject of digital safety at regular intervals, and at least annually.

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

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

12.2 Pupils

All pupils will receive age-appropriate lessons on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering (the use of deception to manipulate individuals into divulging confidential/personal information)
- The risks of removable storage devices (e.g. USBs)

- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to digital safety using CPOMS.

This policy will be reviewed every 2 years (or sooner if necessary) by the Headteacher/DSL. At every review, the policy will be shared with the governing board.

14. Links with other policies

This digital safety policy is linked to other policies including: Child protection and safeguarding policy, Behaviour policy, Staff disciplinary procedures, Data protection policy and privacy notices, Complaints procedure, ICT and internet acceptable use policy, Mobile phones.

Appendix 1: EYFS and KS1 acceptable use agreement

ICT ACCEPTABLE USE AGREEMENT (EYFS & KS1)

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Treat ICT equipment with respect.
• Ask a teacher or adult if I can do so before using them
• Never type or search for anything rude or inappropriate
• Only use websites that a teacher or adult has allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only (or appropriate games at Breakfast or After-School Club)
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never try to use a username or password that does not belong to me
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Log off or shut down a computer or other device when I have finished using it
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed by (Class Members)

Appendix 2: KS2 acceptable use agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR PUPILS AND PARENTS/CARERS

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Tell a trusted adult immediately if I find any material that might upset, distress or harm me or others
- I will be alert to the online risks that I have learnt about, double check things if I am unsure.
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is inappropriate or may upset others
- Log in to devices using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- It will be placed out of view in a pocket or bag as soon as I am within the school grounds
- It will be switched off and handed to an adult as soon as I get to my classroom
- I will not attempt to use or access my device during school time.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor by computer activity and the websites I visit and that there will be consequences if I don't follow the rules.

To be signed by all class members.

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
• I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: 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 /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg 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 / 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 5 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	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 6: Reporting a digital safety incident flowchart