HEDDON-ON-THE-WALL ST. ANDREW'S CE PRIMARY SCHOOL

E-SAFETY POLICY

'Those who walk in wisdom are kept safe.'
Proverbs 28:26

Aims and policy scope

Heddon-on-the-Wall St. Andrew's CE Primary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Heddon-on-the-Wall St. Andrew's CE Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Heddon-on-the-Wall St. Andrew's CE Primary School has a duty to provide the School community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

Heddon-on-the-Wall St. Andrew's CE Primary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Heddon-on-the-Wall St. Andrew's CE Primary School's online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Heddon-on-the-Wall St. Andrew's CE Primary School is a safe and secure environment;
- Safeguard and protect all members of our community online;
- Raise awareness with all members of Heddon-on-the-Wall St. Andrew's CE Primary School's community regarding the potential risks as well as benefits of technology;
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology;
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

The purpose of Heddon-on-the-Wall St. Andrew's CE Primary School's online safety policy is also to:

- Support pupils in understanding that the internet is an integral part of life and to encourage them to think critically about both its positive and negative aspects;
- Foster an environment where pupils can openly discuss how online relationships complement and support meaningful in-person relationships, as well as potential

tensions, such as recognizing that online interactions are not a substitute for high-quality in-person connections;

- Educate pupils on the benefits of limiting time spent online, the risks of excessive screen time, and the impact of online content on their own and others' mental and physical wellbeing;
- Empower pupils to take a critical approach to information and content found online, making responsible decisions about what is appropriate for them and understanding how information is both selected and targeted;
- Ensure that all members of the school community understand that bullying and harassment, including cyberbullying, has a lasting impact upon mental wellbeing, and how to seek help and support.

This policy applies to all staff including the Academy Committee, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.
This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant School Policies including (but not limited to) Safeguarding and Child Protection including Peer on Peer / Child on Child Abuse, Tackling Extremism and Radicalisation, anti-bullying, behaviour, data security, image use, Acceptable Use Policies (appended to this Policy), Mental Health and Wellbeing, Confidentiality, Whistleblowing and relevant curriculum policies including Computing, Personal Social and Health Education (PSHE) and Relationships and Sex Education (RSE) as well as General Data Protection Regulations (GDPR) privacy notices.

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is Mr. Andrew Wheatley
The Online safety (e-Safety) lead for the Governing Body is Mr. Robin Brims

Policy approved by Head Teacher	Mr. Andrew Wheatley	September 2025
Policy approved by the Academy Committee:	Mrs. Michelle Robson	(Chair of Governors)

The date for the next policy review is September 2026

Heddon-on-the-Wall St. Andrew's CE Primary School's Online Safety Policy has been written by the School, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, and the statutory Department for Education guidance on Relationships Education and Relationships and Sex Education, July 2025.

The policy has been approved and agreed by the Leadership Team and Governing Body
The school has appointed the Designated Safeguarding Lead (DSL) Mr. A. Wheatley and deputy DSLs: Mrs. F. O'Reilly and Mrs. H. Abbott as appropriate members of the leadership team and the online safety leads. Mr. D. McDonald is Computing Lead.
The school has appointed Mr. Robin Brims as the member of the Academy Committee to take lead responsibility for online safety (E-Safety).

The online safety (E–Safety) Policy and its implementation will be reviewed by the School at least annually or sooner if required.

1.3 Key responsibilities for the community

1.3.1 The key responsibilities of the School Management and Leadership Team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with National and local recommendations including the latest version of Keeping Children Safe in Education (KCSIE) with appropriate support and consultation throughout the school community;
- Ensuring that online safety is viewed by the whole community as a safeguarding issue with a view that *'It could happen here'* and proactively developing a robust online safety culture;
- Supporting the Designated Safeguarding Leads (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities;
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology;
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material;
- To work with and support technical staff in monitoring the safety and security of school / setting systems and networks and to ensure that the school / setting network system is actively monitored;
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities, including cyber security, and provide guidance regarding safe appropriate communications which reflects the guidance within KCSIE;
- Identify and allocate appropriate information and training for staff and parents through the National Online Safety Portal and ensure this training is completed;
- Ensuring that online safety is embedded within a progressive whole school / setting curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours;
- Ensuring that the curriculum explicitly addresses the concept of privacy and its implications for both children and adults, including the understanding that it is not always right to keep secrets if they relate to being safe;
- Overseeing the integration of curriculum content that educates pupils on the importance of self-respect and how it links to their happiness, and that each person's body belongs to them, distinguishing between appropriate and inappropriate physical and online contact;
- Ensuring the curriculum covers the impact of bullying (including cyberbullying) on mental wellbeing and how to seek help for themselves of others, while also teaching pupils how to judge whether their feelings and behaviour are appropriate and proportionate;
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate;

- Ensure that pupils are explicitly taught about online risks such as video game monetisation, scams, fraud, financial harms and the addictive nature of gaming;
- Incorporating education about health protection, including the importance of sufficient good quality sleep, recommended sleep duration for their age and practical steps such as not using screens in their bedrooms or for an hour before bed, highlighting the impact of poor sleep on weight, mood and learning;
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice;
- Ensuring there are robust reporting channels for the school / setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices;
- To ensure a member of the Academy Committee is identified with a lead responsibility for supporting online safety;
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement;
- To ensure that the Designated Safeguarding Lead (DSL) works with the online safety lead;

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate;
- Keeping up-to-date with current research, legislation and trends regarding online safety;
- Co-ordinating participation in local and National events to promote positive online behaviour, e.g. Safer Internet Day;
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches;
- Work with the school / setting lead for data protection and data security to ensure that practice is in line with current legislation;
- Maintaining a record of online safety concerns / incidents and actions taken as part of the schools safeguarding recording structures and mechanisms;
- Monitor the school’s online safety incidents to identify gaps / trends and use this data to update the school’s education response to reflect need;
- To report to the School Management Team, Academy Committee, Pele Trust and other agencies as appropriate, on online safety concerns and local data / figures;
- Liaising with the Local Authority and other local and National bodies, as appropriate;
- Working with the school / setting leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input;
- Ensuring that online safety is integrated with other appropriate school policies and procedures;
- Meet regularly with the Academy Committee Member with a lead responsibility for online safety.

1.3.3 The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies;
- Reading the school Acceptable Use Policies (AUPs) and adhering to them;
- Taking responsibility for the security of school / setting systems and data;
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care;
- Modelling good practice when using new and emerging technologies;
- Embedding online safety education in curriculum delivery wherever possible;
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures;
- Knowing when and how to escalate online safety issues, internally and externally;
- Being able to signpost to appropriate support available for online safety issues, internally and externally;
- Maintaining a professional level of conduct in their personal use of technology, both on and off site;
- Reading and adhering to policies such as the Pele Trust Code of Conduct, Social Networking Policy and Data Protection Policy;
- To complete online Cyber Security training;
- Demonstrating an emphasis on positive learning opportunities;
- Taking personal responsibility for professional development in this area.

1.3.4 In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised;
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team;
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices;
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL;
- Ensuring that the use of the school / setting's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL;
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised;
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure;
- Report any breaches and liaising with the Local Authority (or other local or National bodies) as appropriate on technical infrastructure issues;
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures;
- Ensuring that the School's ICT infrastructure / system is secure and not open to misuse or malicious attack;

- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices;
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies;
- Reading the school Acceptable Use Policies (AUPs) and adhering to them;
- Respecting the feelings and rights of others both on and offline;
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Understand and applying the principle that people should be respectful in online interactions and that the same principles apply to online relationships and interactions as to face-to-face ones, even when anonymous;
- Consider the impact of their online behaviour on others and displaying respectful conduct when online;
- Learn and apply strategies for resisting peer pressure online and understand the importance of not pressuring others to share information or pictures;
- Develop the ability to critically evaluate online relationships and sources of information, being aware that people sometimes behave differently online, including pretending to be someone they are not, which can lead to dangerous situations;
- Recognising and reporting harmful content or harmful content encountered online;
- Understand and respect the minimum age restrictions for joining social media sites (currently 13+ years in UK) recognising that this protects them from inappropriate content and unsafe contact with older users or strangers;
- Exercise caution about sharing any personal information online and understand how to use privacy and locations settings to protect their data;
- Understand their rights in relation to sharing personal data, privacy and consent online;
- Recognise that each person’s body belongs to them and understanding the differences between appropriate and inappropriate or unsafe physical and online contact;
- Know how to respond safely and appropriately to adults they may encounter online, whether known or unknown, and recognising when a relationship is harmful or dangerous. This will include skills to identify trustworthy individuals;
- Learn about the risks associated with online gaming, video game monetisation, scams, fraud, other financial harms and the potential for gaming addiction and the negative impact this can have;
- Understand the importance of good quality sleep for their health, the amount recommended for their age and practical steps they can take to improve sleep such as avoiding screens in bedrooms and staying off screens for an hour before bed;
- Taking responsibility for keeping themselves and others safe online;
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;

- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading the school Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate;
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home;
- Engaging in open discussions with their children about the nature of online relationships and the critical evaluation of online friendships and sources of information;
- Reinforce with their children an understanding that it is not always right to keep secrets if they relate to being safe and that each person's body belongs to them;
- Discussing the importance of sufficient good quality sleep, including the impact of screen use in the bedroom and before bed with their children;
- Reading and engaging with online safety information from the National Online Safety portal supplied by the school;
- Role modelling safe and appropriate uses of technology and social media;
- Identifying changes in behaviour that could indicate that their child is at risk of harm online;
- Supporting the school in teaching children about the benefits of limiting time spent online, the risks of excessive time on electronic devices;
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns;
- Contributing to the development of the school / setting online safety policies;
- Using School systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE). The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published;
- The Headteacher / Office Manager will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate;
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright;
- Pupils' work will be published with their permission;
- The administrator account for the school website will be safeguarded with an appropriately strong password;
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing images and videos online

- The School will ensure that all images and videos shared online are used in accordance with the School Image Use Policy;
- The School will ensure that all use of images and videos take place in accordance other policies and procedures including General Data Protection Regulations (GDPR), Data Security, Acceptable Use Policies, Codes of Conduct, Social Media, Use of Personal Devices and mobile phones etc;
- In line with the Image Policy, written permission from parents or carers will always be obtained before images / videos of pupils are electronically published.

2.3 Managing E-mail

- Pupils may only use School provided e-mail accounts for educational purposes;
- All members of staff are provided with a specific School Google Mail e-mail address to use for any official communication;
- The use of personal e-mail addresses by staff for any official School business is not permitted;
- The forwarding of any chain messages / e-mails etc. is not permitted. Spam or junk mail will be blocked and reported to the e-mail provider;
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email;
- Access to School e-mail systems will always take place in accordance to data protection legislation and in line with other appropriate School policies e.g. Confidentiality;
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the School Safeguarding files / records;
- Whole class or group e-mail addresses may be used for communication outside of the School;
- Staff will be encouraged to develop an appropriate work life balance when responding to e-mail;
- Staff will not communicate with either parents or children via their School or personal e-mail accounts. Parental e-mail communication must take place via the School Admin, SEND or home learning e-mail addresses for the child’s year group;
- Excessive social e-mail use can interfere with teaching and learning and will be restricted. Access in school to external personal e-mail accounts may be blocked;
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on School headed paper would be;
- School e-mail addresses and other official contact details will not be used for setting up personal social media accounts;
- Staff School e-mails must all contain the approved GDPR footer within the electronic signature;
- Staff will follow the Pele Trust Social Networking and Data Protection Policies.

2.4 Official video-conferencing and webcam use for educational purposes:

- The school acknowledges that video-conferencing / live streaming is a challenging activity with a wide range of learning benefits as seen during the COVID-19 pandemic. Preparation and evaluation are essential to the whole activity;
- The Headteacher will direct when it is appropriate to carry out video-conferencing or live streaming and consent must be sought prior to arranging either activity;
- The school will video conference using Google Meet, although there may be times when attending external events when platforms such as Microsoft Teams or Zoom may be used;
- The school will only use video-conferencing when necessary eg: providing remote education to isolating pupils such as story-telling sessions or in the event of a National lockdown; to enable classes to meet for whole school events such as Collective Worship and Hymn Practice when it is not possible to do so and for work with our Partner Schools across Europe. When joining a meeting both video camera and microphone will be turned off until meeting has begun;
- Video-conferencing may only take place through school equipment eg: laptop, desktop or Chromebook;
- Joining codes for meetings will not be posted publicly but shared via Google Classroom or via SchoolComms for children in Year 1 and via Tapestry for children in Early Years;
- All people attending must display their own name using the software;
- Staff will carry out a risk assessment prior to carrying out video-conferencing or live streaming;
- Should the meeting be joined by someone who was not on the invitation list they will be blocked by the meeting administrator and the incident will be reported to the DSL / Online Safety Officer;
- For further details about the use of video conferencing for the purposes of Remote Education please see the parental information of Remote Education on the School website.

Users

- Parent / carer consent will be sought prior to children taking part in video-conferencing or live streaming;
- Pupils must be appropriately dressed and in an appropriate space if they are joining from home (eg when isolating or during National lockdown);
- If joining from home, pupils may be supervised by parents, however, parents are not to join in or make comments during the session unless invited to do so by the class teacher;
- Unless they are speaking participants will mute their microphones but will leave their cameras on;
- Video-conferencing will be appropriately supervised if taking place in school;

Content

- Participants are not permitted to record the stream unless this has been agreed prior to the meeting. The reason for recording must be clearly established and this should be clear to and agreed by all participants prior to recording. Recorded material is subject to GDPR and should be stored securely in line with the school retention schedule;

- If third party materials are to be used the school will check that recording is acceptable to avoid infringing third party intellectual property rights;
- If it is an external third party leading the session the school will establish that what is being delivered is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet and any associated devices.

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information;
- The School's internet access will be designed to enhance and extend education;
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils;
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential;
- Supervision of pupils will be appropriate to their age and ability

    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability;
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability;
    - Secondary, sixth form and college pupils will be appropriately supervised when using technology, according to their ability and understanding.

- All School owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place;
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- The school will use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community;
- The School will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information;
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- Pupils will be taught how data and information is shared and used online, and their rights regarding personal data, privacy and consent in an age appropriate manner;
- Pupils will be explicitly taught that each person's body belongs to them and if anyone online or offline makes them uncomfortable or scared with their touch or words they will tell a trusted adult;

- Pupils will be taught about why certain social media, apps and games are age restricted;
- The curriculum will explore the positive and negative aspects of the internet including the benefits of limiting screen time, along with the risks of excessive use of mental and physical wellbeing;
- Pupils will be taught how to recognise and report feelings of being unsafe or feeling bad about any adult; how to ask for advice or help for themselves or others with confidence using appropriate vocabulary; and to keep trying until they are heard;
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum;
- The School will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of School Learning Platforms / Portals / Gateways

The School uses the following Learning Platforms with pupils:

- Purple Mash;
- Read, Write Inc Portal;
- White Rose Maths;
- Timetables Rockstars;
- Sumdog;
- Google Classroom;

The School uses the Tapestry Platform as a tool to share progress with parents in Early Years.

National Online Safety Portal is also used with parents but this is a repository of information with no options to upload or alter content on the platform.

The following applies to the use of all Learning Platforms that the school uses:

- Leaders / managers and staff will regularly monitor the usage of the Learning Platforms (LPS) in all areas, in particular message and communication tools and publishing facilities;
- Pupils / staff will be advised about acceptable conduct and use when using Purple Mash and Google Classroom;
- Only members of the current pupil, parent / carers and staff community will have access to the LPS;
- All users will be mindful of copyright issues and will only upload appropriate content onto the LPS;
- When staff, pupils' etc leave the school their account or rights to specific school areas will be disabled;
- Any concerns about content on the LPS will be recorded and dealt with in the following ways:
  - ➢ The user will be asked to remove any material deemed to be inappropriate or offensive;
  - ➢ The material will be removed by the site administrator if the user does not comply;
  - ➢ Access to the LPS for the user may be suspended;
  - ➢ The user will need to discuss the issues with a member of leadership before reinstatement. eg: A pupil's parent/carer may be informed;

- A visitor may be invited onto the LPS by a member of the leadership. In this instance there may be an agreed focus or a limited time slot;
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3. Social Media Policy

3.1. General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Heddon-on-the-Wall St. Andrew's CE Primary School community and exist in order to safeguard both the School / setting and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video / photo sharing sites, chatrooms, instant messenger and many others;
- All members of Heddon-on-the-Wall St. Andrew's CE Primary School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times;
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community;
- All members of Heddon-on-the-Wall St. Andrew's CE Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others;
- The School will control pupil and staff access to social media and social networking sites whilst on site and when using School provided devices and systems;
- The use of social networking applications during school hours for personal use **is not** permitted;
- Any concerns regarding the online conduct of any member of the Heddon-on-the-Wall St. Andrew's CE Primary School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as Allegations against Staff, Safeguarding and Child Protection including Child on Child Abuse, Tackling Extremism and Radicalisation, anti-bullying, and behaviour.
- Any breaches of School policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as Allegations against Staff, Safeguarding and Child Protection including Child on Child Abuse, Tackling Extremism and Radicalisation, anti-bullying, and behaviour.

3.2 Official use of social media

Heddon-on-the-Wall St. Andrew's CE Primary School official social media channels are:

Twitter, Facebook and Blogs

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement;
- Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher;
- Official School social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes;
- Staff will use School provided e-mail addresses to register for and manage any official approved social media channels;
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation;
- All communication on official social media platforms will be clear, transparent and open to scrutiny;
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc;
- Official social media use will be in line with existing policies including Safeguarding and Child Protection including Child on Child Abuse, Tackling Extremism and Radicalisation, anti-bullying;
- Images or videos of children will only be shared on official social media sites / channels in accordance with the Image Use Policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community;
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible / appropriate, run and / or linked to from the school website and take place with written approval from the Leadership Team;
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence;
- Parents / Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community;
- Public communications on behalf of the School will, where possible, be read and agreed by at least one other colleague;
- Blog posts for classes where there are children for whom there is no image use consent will be written and saved as drafts and then thoroughly checked by the Headteacher or member of the Senior Management Team prior to being posted. These posts will then be posted by the Headteacher or member of the Senior Management Team;
- Official social media channels will link back to the School website and / or Acceptable Use Policy to demonstrate that the account is official;
- The School will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff Use of Social Media

- Staff will adhere to the Pele Trust Social Networking Policy.

3.5 Pupils’ use of Social Media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy;
- Pupils will be encouraged to consider the impact of their online behaviour on others and to consistently display respectful behaviour online;
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes;
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real / full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends / family, specific interests and clubs etc. They will be taught how to use privacy settings and location settings effectively to protect their personal information;
- Pupils will be advised not to meet any online friends without a parent / carer or other responsible adult’s permission and only when they can be present;
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications;
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private / protected;
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required;
- Any official social media activity involving pupils will be moderated by the School where possible;
- The School is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age. The School is clear on the emotional damage that can be done by accessing age inappropriate apps and materials;
- Discussions will take place with pupils about the reasons for age restrictions on social media, apps, computer / video games, and online gaming, including gambling sites with a focus on protecting themselves from inappropriate content or unsafe contact;
- Pupils will be made aware of the risks associated with online gambling, video game monetisation, scams, fraud and other financial harm, including gambling addiction, which may be associated with social media sites;
- The curriculum will reinforce to pupils that once a picture or words have been shared online there is no way of deleting it everywhere, and the pupils have no control over where it ends up;
- Pupils will be taught strategies for resisting peer pressure to share information or images online;
- Any concerns regarding pupils’ use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying, and behaviour;
- Any concerns regarding pupils’ use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents / carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding Personal Devices and Mobile Phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the Heddon-on-the-Wall St. Andrew’s CE Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.

- Heddon-on-the-Wall St. Andrew’s CE Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents / carers but requires that such technologies need to be used safely and appropriately within schools.

4.2 Expectations for the safe use of Personal Devices and Mobile Phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies;
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual;
- Mobile phones and personal devices are not permitted to be used in certain areas within the school;
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Discipline / Behaviour policy;
- All members of Heddon-on-the-Wall St. Andrew’s CE Primary School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage;
- All members of Heddon-on-the-Wall St. Andrew’s CE Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the School / settings policies.

4.3 Pupils’ use of Personal Devices and Mobile Phones

- Only pupils who are in Upper Key Stage 2 (Years 5 and 6) and who are walking to and from school themselves are permitted to bring mobile phones to school. These are turned off and handed in to the Class teacher at the beginning of the day and stored in a locked cupboard in the Office. They are handed back to pupils at the end of the day. Pupils are not allowed access to their mobile phone during the school day.
- Pupils in other year groups are not permitted to bring / use mobile phones or personal devices in School as they are not allowed to walk to and from school themselves. If a pupil brings a phone or device to School then the phone or device will be confiscated and

will be held in a secure place in the School Office. Mobile phones and devices will be released to parents / carers;

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones;
- All use of mobile phones and personal devices by children will take place in accordance with the Acceptable Use Policy;
- If a pupil needs to contact his / her parents / carers they will be allowed to use a School phone;
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the School Office via telephone or the admin email;
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences;

4.4 Staff use of Personal Devices and Mobile Phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with the Headteacher / line manager;
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose;
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons / educational activities;
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc;
- Staff personal mobile phones and devices will be switched off / switched to ‘silent’ mode during lesson times;
- Bluetooth or other forms of communication should be “hidden” or switched off during lesson times;
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances;
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations;
- If a member of staff breaches the School Policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted;
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the School Allegations Management Policy.

4.6 Visitors use of personal devices and mobile phones

- Parents / carers and visitors must use mobile phones and personal devices in accordance with the school’s Acceptable Use Policy;
- Use of mobile phones or personal devices by visitors and parents / carers to take photos or videos must take place in accordance with the school Image Use Policy;

- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use;
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Heddon-on-the-Wall St. Andrew's CE Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace;
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed;
- The School will ensure that appropriate filtering and monitoring systems (Lightspeed filtering and Senso Cloud) are in place to prevent staff and pupils from accessing unsuitable or illegal content. The school will work with Northumberland Local Authority and the Schools Broadband team to ensure that filtering is continually reviewed;
- The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device;
- The School will audit technology use to establish if the online safety (E–Safety) Policy is adequate and that the implementation of the policy is appropriate;
- Methods to identify, assess and minimise online risks will be reviewed regularly by the School Senior Management Team.

5.2. Internet use throughout the wider School / setting community

- The School will provide an Acceptable Use Policy for any guest / visitor who needs to access the school computer system or internet on site.

5.3 Authorising internet access

- The School will maintain a current record of all staff and pupils who are granted access to the school's devices and systems;
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources;
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability;
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate;
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety (E-Safety) curriculum is established and embedded throughout the whole School, to raise awareness regarding the importance of safe and responsible internet use amongst pupils;
- This is based upon the ‘SMART’ rules:
    - Safe;
    - Meet;
    - Accept;
    - Reliable;
    - Tell.
- Education about safe and responsible use will precede internet access;
- Pupils’ input will be sought when writing and developing School online safety policies and practices, including curriculum development and implementation;
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability;
- All users will be informed that network and Internet use will be monitored;
- Online safety (E-Safety) will be included in the PSHE and Computing programmes of study, covering both safe School and home use;
- Online safety (E-Safety) education and training will be included as part of the transition programme across the Key Stages and when moving between establishments;
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access;
- CEOP reporting and Childline information is posted in all rooms with Internet access;
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas;
- External support will be used to complement and support the school’s internal online safety (E-Safety) education approaches;
- The School will reward positive use of technology by pupils.

6.2 Engagement and education of children and young people considered to be vulnerable

- Heddon-on-the-Wall St. Andrew’s CE Primary School is aware that some children may be considered to be more vulnerable online due to a range / combination of factors;
- Heddon-on-the-Wall St. Andrew’s CE Primary School will ensure that differentiated and ability appropriate online safety (E-Safety) education is given, with input from specialist staff as appropriate (e.g. SENDCO, Looked after Child Co-ordinator).

6.3 Engagement and Education of Staff

- The online safety (E-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities;
- All staff will complete the following training annually:

  - ➢ Northumberland Online Safety Support annual training;
  - ➢ Cyber Security (not an annual requirement);
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using School systems and devices;
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular basis;
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities;
- Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns;
- The School will highlight useful online tools which staff should use according to the age and ability of the pupils;
- Academy Committee Members will be expected to complete the Annual Certificate in Online Safety for Governors to ensure that they are fully aware of the work the School is doing and to enable them to effectively monitor the actions of the School.

6.4 Engagement and Education of Parents and Carers

- Heddon-on-the-Wall St. Andrew's CE Primary School recognises that parents / carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology;
- Parents' attention will be drawn to the school online safety (E-Safety) policy and expectations in newsletters, letters and on the school website;
- A partnership approach to online safety at home and at School with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, school fairs and sports days;
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Safety on the Internet and Responsible Use of Computers Contract and discuss its implications with their children;
- Information and guidance for parents on online safety will be made available to parents in a variety of formats. This includes providing access to resources including help sheets, guides, videos and training courses via the National Online Safety portal;
- #WakeUpWednesday where online safety information is shared via social media;
- Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations and Data Protection Act 1998;

- Full information regarding the school's approach to data protection and information governance can be found on the School website GDPR section and in the schools Information Security Policy.

7.2 Security and Management of Information Systems

- The security of the School information systems and users will be reviewed regularly;
- Virus protection will be updated regularly;
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems such as Google Drive;
- Portable media may not be used in school;
- Unapproved software will not be allowed in work areas or attached to e-mail;
- Files held on the school's network will be regularly checked;
- The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users;
- All users will be expected to log off or lock their screens / devices if systems are unattended;
- The School will log and record internet use on all school owned devices.

7.2.1 Password Policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time;
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it;
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private;
- From Year 1, all pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private;
- We require staff and pupils to use **STRONG** passwords for access into our system. Pupil passwords are pre-generated by Northumberland County Council.

7.3 Filtering and Monitoring

- The Academy Committee will ensure that the School has age and ability appropriate filtering and monitoring in place whilst using School devices and systems to limit children's exposure to online risks;
- The School's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff;
- All monitoring of School owned / provided systems will take place to safeguard members of the community;

- All users will be informed that use of School systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation;
- The School uses educational filtered secure broadband connectivity through Northumberland County Council Broadband SLA which is appropriate to the age and requirement of our pupils;
- The School uses the Fortinet filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc. For further details about Fortinet please click here;
- The School uses Senso Cloud monitoring software. The DSL receives a report of all potential breaches weekly. Screenshots of potential breaches are examined and reviewed. The DSL logs the status of all screenshots on the system. For further details about Senso Cloud please click here;
- The School will work with Northumberland County Council and the Schools Broadband team to ensure that filtering policy is continually reviewed;
- The School will have a clear procedure for reporting breaches of filtering which all members of the School community (all staff and all pupils) will be made aware of;
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate;
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list;
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Management Team;
- The Senior Management Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate;
- Any material that the School believes is illegal will be reported to appropriate agencies such as Internet Watch Foundation, Northumbria Police or CEOP immediately;
- Both Fortinet and Senso Cloud meet the Department for Education filtering and monitoring standards.

7.4 Management of Applications (apps) used to record Children's Progress

- The Headteacher is ultimately responsible for the security of any data or images held of children;
- Apps / systems which store personal data will be risk assessed prior to use;
- All apps / systems that the School uses are compliant with GDPR regulations and have an identified privacy notice;
- Only School issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images;
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft;
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc;
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

8. Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, up-skirting, sexual harassment, online / cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils;
- All members of the School community will be informed about the procedure for reporting online safety (E-Safety) concerns, such as breaches of filtering, sexting, up-skirting, sexual harassment, cyberbullying, illegal content etc;
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (E-Safety) incidents involving child protection concerns, which will then be recorded on CPOMS (in line with the Pele Trust CPOMS Handbook);
- Reporting procedures will be clearly communicated for all forms of online abuse, bullying and harassment emphasising where and how to seek support from trusted adults;
- Through Relationships and Sex Education (RSE) and E-Safety curriculum the school will ensure pupils are equipped with the vocabulary and confidence to report concerns or abuse and to seek advice or help for themselves or others. This will include resilience to keep trying until their voice is heard;
- When responding to online incidents, the school will consider the specific impact on pupils' mental wellbeing, recognising that bullying (including cyberbullying) and other online harms can have negative and lasting effects. Support will be offered to pupils (both victims and perpetrators (if applicable)) to help understand and manage their feelings and behaviours in response to such incidents;
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Northumberland Strategic Safeguarding Partnership (NSSP) thresholds and procedures;
- Complaints about Internet misuse will be dealt with under the School's complaints procedure;
- Complaints about online / cyber bullying will be dealt with under the School's Anti-Bullying Policy and Procedure;
- Any complaint about staff misuse will be referred to the Headteacher;
  Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer – Louise Prudhoe- **07500 606174** (Monday to Thursday 08:30-17:00, Friday 08:30-16:30) or **01670 536400** (Out of hours) LADO@northumberland.gov.uk
  Make a Referral: complete Online Referral Form - Using the online referral form helps to ensure information can be responded to in a timely manner.
- Pupils, parents and staff will be informed of the School Complaints Procedure;
- Staff will be informed of the Complaints and Whistleblowing Procedure;
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns;
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community;
- The school will manage online safety (E-Safety) incidents in accordance with the school Discipline / Behaviour Policy where appropriate;

- The school will inform parents / carers of any incidents of concerns as and when required;
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required;
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Northumberland Strategic Safeguarding Partnership or Northumbria Police via 101 or 999 if there is immediate danger or risk of harm;
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Northumbria Police;
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Northumberland Safeguarding Team;
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Northumberland Strategic Safeguarding Partnership to communicate to other schools in Northumberland;
- Parents and children will need to work in partnership with the school to resolve issues.

9.0 Monitoring and Review

This policy and procedure will be monitored and reviewed annually by the full Academy Committee. Where there are issues with the way the policy and / or procedure are working, these will be looked at closely with a view to identifying measures to improve their effectiveness.

Document Record

Version	Reason for Amendments/Update/Review	Date of Adoption by School	Date of next review
1.0	Policy rewritten to ensure compliance with DfE Relationships, Sex and Health Education statutory guidance (2025) and Relationships Education guidance (Primary) (2025)	09.09.2025	08.09.2026

Appendix 1: Pupil Acceptable Use Policy in Key Stage 1

Acceptable Use Policy for Children in Key Stage 1

I want to feel safe all the time.

I agree that I will:

Always keep my passwords a secret;
Only open pages which my teacher has said are ok;
Only work with people I know in real life;
Remember that my body belongs to me and if anyone, online or offline, makes me feel scared or uncomfortable with their touch or words I will tell a trusted adult;
Understand that it is important to tell an adult a secret if it is about keeping me or others safe;
Make sure all messages I send are polite;
Show my teacher if I get a nasty message;
Not reply to any nasty message or anything which makes me feel uncomfortable;
Not give my mobile phone number to anyone who is not a friend in real life;
Only email people I know or if my teacher agrees;
Only use my school email;
Talk to my teacher before using anything on the internet;
Not tell people about myself online (I will not tell them my name, anything about my home, family or pets);
Not upload photos of myself without asking a teacher;
Never agree to meet a stranger;
Ask a grown-up if I can use a game or app and understand why some games and apps are only for older children;
Make sure to have a good night’s sleep and not use screens in my bedroom before bed.

Anything I do on the computer may be seen by someone else.
I am aware of the CEOP report button and know when to use it.

Signed	
Name (in block capitals)	
Class	
Date	

Appendix 2: Pupil Acceptable Use Policy in Key Stage 2

Acceptable Use Policy for Children in Key Stage 2

I want to feel safe all the time.

I agree that I will:

Always keep my passwords a secret;

Only use, move and share personal data securely;

Only visit sites which are appropriate;

Think critically about what I see and read online and make responsible decisions about content;

Work in collaboration only with people my school has approved and will deny access to others;

Respect the school network security;

Make sure I am always respectful online and think about how my behaviour affects others;

Remember that my body belongs to me and if anyone, online or offline, makes me feel scared or uncomfortable with their touch or words I will tell a trusted adult;

Show a responsible adult any content that makes me feel unsafe or uncomfortable;

Know that it is not always right to keep secrets if they are about being safe and I will seek help and keep trying until I am heard;

Not reply to any nasty message or anything which makes me feel uncomfortable;

Not to use my own mobile device in school unless I am given permission;

Only give my mobile phone number to friends I know in real life and trust;

Only email people I know or approved by the school;

Always follow the terms and conditions when using a site;

Always keep my personal details private (my name, family information, the journey to school, my pets and hobbies are all examples of personal details);

Understand that I have rights about sharing my personal data, privacy and giving consent online;

Learn to use privacy and location settings on devices and apps to protect my personal information;

Always check with a responsible adult before I share images of myself or others;

Never meet with an online friend without taking a responsible adult that I know with me.

Recognise when a relationship (online or offline) is harmful or dangerous and use my skills to decide who to trust and who not to trust;

Understand why some social media, apps and games have age restrictions and respect these rules;

Prioritise good quality sleep, knowing how much I should get for my age and avoid using screens in my bedroom to help me sleep better. I am aware of the CEOP report button and know when to use it. I know that anything I share online may be monitored. I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.	
Signed	
Name (in block capitals)	
Class	
Date	

Appendix 3: Acceptable Use Policy for any Adult working with Children

Acceptable Use Policy for any Adult working with Children

The policy aims to ensure that any communication technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

Only use, move and share personal data securely;
Respect the school's network security;
Implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources;
Respect the copyright and intellectual property rights of others;
Only use approved email accounts;
Only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site;
Only give permission to pupils to communicate online with trusted users;
Use ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues;
Not use or share my personal (home) accounts / data (eg Whatsapp, Facebook, email, eBay, Amazon etc) with pupils;
Set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted symbols);
Report unsuitable content and / or ICT misuse to the DSL / deputy DSLs or Online Safety Officer;
Complete any online safety training, including cyber security, as designated by the school.

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.
I understand that school strongly advises that settings on all social media sites should be kept to private. I am mindful about who can see my page and any followers and friends that I have that are linked to the school.

I agree that I will not:

Visit internet sites, make, post, download, upload inappropriate images or pass on material, remarks, proposals or comments that brings the school into disrepute containing or related to: promoting discrimination of any kind; promoting violence or bullying; promoting racial or religious hatred; promoting illegal acts or images that could be deemed to be sexualized or provocative;
Do anything which exposes others to danger;
Post any other information which may be offensive to others;
Forward chain letters;
Breach copyright law;
Use personal digital recording equipment including cameras, phones or other devices for taking / transferring images or audio of pupils or staff without permission;
Store images or other files off-site without permission from the Headteacher.

I will ensure that any private social networking sites, blogs etc that I create or actively contribute to, do not compromise my professional role.

I understand that the data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school’s management information system or CPOMS online recording system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed	
Name (in block capitals)	
Class	
Date	

Appendix 3: E-Safety Letter Template to Parents (to be sent on headed paper)

Parent / Carer Name	
Pupil Name	
Class	

Dear Parent / Carer,

As the parent or legal guardian of the above child(ren), I grant permission for my child to have access to use the internet, Purple Mash online platform, Google Classroom, school email and other ICT facilities at school.

I know that my child has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my child may be informed if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to emails, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the internet sites they visit. I also know that the school may contact me if there are concerns about my child's e-safety or online behaviour.

I understand the school's commitment to teaching my child about the importance of critically evaluating online relationships / friendships and information and the risks associated with people they have only met online.

I will support my child in understanding that it is not always right to keep secrets if they relate to being safe; that their body belongs to them; and in distinguishing between appropriate and inappropriate content.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I acknowledge the importance of discussing with my child the benefits of limiting time spent online; the risks of excessive screen time; and the impact of online content on their mental and physical wellbeing.

I will encourage healthy sleep habits for my child, including avoiding screen time in the bedroom for an hour before bed.

I am aware that the school permits parents / carers to take photographs of their own children at designated times at school events. I also understand that the school does not permit the taking of video footage or photos during events as there are a number of children for whom there is no image permission for safeguarding reasons and to share such images online would put them at significant risk of harm.

I will support the school's approach to e-safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of our school community.

Parent / Carer Signature	
Parent / Carer Name (Block Capitals)	
Date	