Richard Coates
CE Primary School



Online Safety and Acceptable Use Policy

Implemented October 2026
Review date- October 2027

PELE TRUST

Richard Coates CE Primary School is part of Pele Trust.

Richard Coates CE Primary School

Scope of the policy

This policy is applicable to staff, volunteers, pupils and all visitors to Richard Coates CE Primary School. This policy should be read alongside Richard Coates CE's policies and procedures on child protection and safeguarding. It reflects Keeping Children Safe in Education 2026 (KCSIE), which came into force on 1 September 2026, the DfE filtering and monitoring standards, the DfE Generative AI: product safety standards and the DfE statutory guidance on mobile phones in schools.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Purpose

The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Provide staff, volunteers and parents with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Richard Coates' activities.

Richard Coates CE Primary School

Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is James Watson

The Deputy Designated Safeguarding Leads are Lucy Fargher, Laura Tweddle, Steph Brogden and Samantha Rutter

The Safeguarding leads (including Online Safety) for the Academy Committee are Melanie King and Kate Richards.

The Online Safety Coordinator is Zoe Wilson

Policy approved by the Academy Committee: Melanie King (Chair of Governors)

The policy has been approved and agreed by the Leadership Team and Academy Committee

The Online Safety (E–Safety) Policy and its implementation will be reviewed by the school on an annual basis. The DSL and Online Safety Coordinator also complete an annual review of the school's wider approach to online safety alongside this policy review, using a recognised self review tool. The review is recorded, its findings feed into the school's safeguarding action plan and a summary is shared with the Academy Committee through the Headteacher's report.

Responding to complaints

- The school will take all reasonable precautions to ensure online safety. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school (nor Pele Trust) can accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour Policy.
- Our online safety coordinator team, James Watson and Zoe Wilson are the first points of contact for any complaint. Any complaint about staff misuse will be referred to the Headteacher.

- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the school's child protection procedures.

We believe that:

- Children and young people should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges
- In line with KCSIE 2026, online risks fall into four areas. Content: being exposed to illegal, inappropriate or harmful content, including AI generated content and misinformation. Contact: being subjected to harmful online interaction with other users, including through AI chatbots and companions. Conduct: online behaviour that increases the likelihood of, or causes, harm, such as creating or sharing nudes, semi nudes or AI generated (deepfake) images. Commerce: risks such as online gambling, inappropriate advertising, phishing and scams.
- Online and offline risks are often linked. Abuse between children can happen online, inside and outside school, and the absence of reports does not mean that it is not happening.
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- We have a responsibility to help keep children and young people safe online, whether or not they are using Richard Coates's network and devices
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- Appointing an online safety coordinator (Zoe Wilson).
- Providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults (AUP)
- Supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- Supporting and encouraging parents and carers to do what they can to keep their children safe online, including the use of a parent acceptable use policy (AUP)
- Developing an online safety agreement for use with young people and their parents/carers, with an age appropriate version for younger pupils
- Developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- Reviewing and updating the security of our information systems regularly, including against the DfE cyber security standards for schools and colleges
- Ensuring that usernames, logins, email accounts and passwords are used effectively
- Ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- Providing supervision, support and training for staff and volunteers about online safety
- Examining and risk assessing any social media platforms and new technologies, including generative AI tools, before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- Having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sending

of nudes and semi-nudes, AI generated or manipulated images, sexual abuse and sexual exploitation
- Making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- Reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Education and curriculum

The school has a clear, progressive online safety education programme primarily as part of the computing curriculum but this is also referenced in all areas of school life (including PSHE). Our Relationships and Health Education (RHE) curriculum has been updated from September 2026 in line with the DfE 2025 statutory guidance. It covers a range of skills and behaviours appropriate to children's ages and experience, including:

- Digital literacy including critical thinking and identifying misinformation online.
- Understanding what AI is, that AI generated content may be inaccurate or fake, and that AI chatbots are not people.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Recognising and reporting concerns or abuse.
- Positive relationships, including recognising manipulation, pressure and coercion online at an age appropriate level.
- Laws around online behaviour (Prevent Duty and Sharing Nudes and Semi-Nudes Guidance for schools)

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind children about their responsibilities using the Acceptable Use Agreement
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.

- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.
- Annual staff and governor training, including filtering and monitoring, how to report a filtering concern and what to do if harmful content is seen, and the safeguarding risks of AI
- Safe delivery of remote learning when the school is closed or students are accessing lessons remotely.

Artificial intelligence

KCSIE 2026 recognises artificial intelligence as a safeguarding issue. The school will:

- Only use generative AI tools that have been approved by the Headteacher and risk assessed against the DfE Generative AI: product safety standards, including filtering, monitoring and reporting, data protection and age restrictions.
- Ensure pupils only use generative AI in school with close supervision and through tools with appropriate filtering and monitoring.
- Ensure that personal data about pupils, families or staff is never entered into generative AI tools unless the tool has been approved for that purpose and a data protection impact assessment is in place.
- Review filtering and monitoring arrangements whenever a new AI tool is introduced.
- Treat the creation or sharing of AI generated sexual or indecent images of children (deepfakes or nudification) as a safeguarding concern. These incidents will be managed by the DSL in line with the Child Protection Policy, KCSIE Part 5 and the UKCIS sharing nudes and semi nudes guidance, and images will never be viewed, copied or forwarded by staff.
- Follow the DfE guidance on generative AI in education and keep staff updated as guidance changes.

The school will ensure that:

- Staff are provided with updated information on how the GDPR and Data Protection Act affect the way data is collected and stored at school.
- Staff understand the requirements of the GDPR and Data Protection Act in terms of sending and receiving sensitive personal information.

- All sensitive and confidential information should be securely stored and password protected.
- Regular training is available to staff on online safety issues and the school's online safety education programme.
- Information and guidance on the Safeguarding policy (including updates to Prevent Duty guidance and Keeping Children Safe in Education) and the school's Acceptable Use Policy is provided to all staff and governors at least annually (see appendices).

Parent engagement

The school recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the school in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends. The Friday Flyer responds to trends identified through our monitoring system and shares weekly online safety parent guides.
- Face to face or online sessions to support parents in developing their child's/children's digital resilience, with at least one parent online safety session each year
- Opportunities to share in their children's online safety learning (e.g. worships, performances)
- Support and advice on online safety for their children outside of school through the use of Parent Zone, Thinkuknow and Interland (Google)
- Clear information on our phone free school day and how parents can support it at home.
- The Parent Code of Conduct, which sets out our expectations for respectful use of social media in relation to the school community.
- Signposting to further resources and websites.

Conduct and Incident management

Conduct:

All users are responsible for using the school ICT systems in line with the Acceptable Use Agreements. They should understand the consequences of misuse, or accessing inappropriate materials.

All members of the school community should know that this policy also covers their online activity outside of school if it relates to their membership of the school.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in school, by signing an Acceptable Use Agreement. They will also be given clear information about the consequences that might result from misuse.

Incident Management:

All members of the school community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the school policy. The school actively seeks advice and support from external agencies in handling online safety issues. Parents and carers will be informed of any online safety incidents relating to their own children, unless doing so may put the child at risk. All parents and carers will receive more general online safety advice in response to incidents, without revealing any sensitive or personal information about children.

All online safety concerns are recorded on CPOMS using the online safety category, with the actions taken and the outcome. Online child on child abuse is managed in line with KCSIE Part 5 and the Behaviour and Anti-Bullying Policies. The DSL analyses online safety incidents and filtering and monitoring alerts for patterns and reports a summary to the Academy Committee each term through the Headteacher's report.

Managing the ICT infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are

implemented. It will also ensure that the relevant people will be effective in carrying out their online safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the school meets recommended technical requirements, including the DfE digital and technology standards and the cyber security standards for schools and colleges.
- There will be regular reviews and audits of the safety and security of the school's technical systems.
- All users will have clearly defined access rights to the technical systems and school owned devices.
- Users of ICT systems log in with usernames and passwords
- The administrator passwords for the school ICT system, used by the Network Manager, are also available to the Headteacher and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school allows different filtering levels for groups of users – staff / students.
- The school regularly monitors and records the activity of users on the school technical systems and this extends to the use of school-owned devices when being used remotely and users are made aware of this in the Acceptable Use Agreement.
- Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Filtering and Monitoring

- The Academy Committee will ensure that the school has age and ability appropriate filtering and monitoring systems in place whilst using school devices and systems to limit children's exposure to online risks;

- The DSL takes lead responsibility for filtering and monitoring, working with the IT provider. The Academy Committee safeguarding lead holds strategic responsibility and checks that the standards are met.
- 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 Senso Cloud monitoring alongside its filtering system, which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc;
- 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;
- A named Deputy DSL completes the weekly monitoring review when the DSL is absent. Review dates and actions are recorded;
- The school will work with Northumberland County Council and the Schools Broadband team to ensure that filtering policy is continually reviewed;
- Filtering and monitoring provision is reviewed at least annually against the DfE filtering and monitoring standards by the DSL, the IT provider and the Academy Committee safeguarding lead. The review considers where AI tools are used and whether the system can manage real time and AI generated content. A record of the review and the checks made is kept as evidence;
- Filtering is tested each term (for example using the SWGfL test site) and the results are recorded;
- An additional review takes place when there is a safeguarding concern, a change in working practice or new technology is introduced, including any new generative AI tool;
- 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;
- To support schools to meet their duty, the Department for Education has published filtering and monitoring standards.

Equipment and Digital Content

Use of Mobile Technologies

Personal mobile phones and mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal mobile phones or other internet enabled devices which are brought into school.

Richard Coates is a mobile phone free school by default, in line with the DfE statutory guidance on mobile phones in schools and KCSIE 2026. Pupils do not have access to mobile phones or similar devices at any point in the school day, including lessons, break times and lunchtimes, on the school site.

Student Use

Pupils should only bring a mobile phone to school if they need it for travelling to and from school, with the agreement of their parents. Phones must be switched off and handed in at the start of the day to be stored securely, and are collected at home time. If a student breaches the school policy, then the phone or device may be confiscated and will be held in a secure place in the school office. Mobile phones

and devices will be released to parents or carers in accordance with the school policy.

This also includes the use of smart watches, smart glasses and any other connected device (or anything which can connect to mobile data). These devices must not be used to message, photograph or record during the school day. Students will be reminded not to bring these items to school. If this policy is breached, then the device will be taken from the student and kept at the school office. Parents will also be notified.

Any exception, for example where a pupil needs a device to manage a medical condition, will be agreed with parents, recorded in the pupil's individual healthcare plan and reviewed regularly.

Staff Use

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Staff devices such as iPads are PIN protected and only used for school purposes.

Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team. Staff model our phone free culture by not using personal phones for personal reasons in front of pupils.

Staff should not use their own devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

Where staff are required to use a mobile phone for school duties – e.g. in case of emergency during off-site activities, or for contacting students or parents - then a school mobile phone will be provided. In an emergency where staff do not have access to a school device, they should use their own device and hide their own number (by dialing 141 first).

Visitors, volunteers and contractors are told on arrival, through the visitor leaflet, that personal phones must not be used in areas where children are present and must never be used to take photographs of children.

Photography and Image Sharing Guidance

Digital images and video

We will seek permission from parents and carers for the use of digital photographs or video involving their child as part of the Use of Digital and Video Images Agreement when their child joins the school. Parents are presented with a range of options which include how these images may be used, e.g. promotional material, school website, external partners etc

We do not identify pupils in online photographic materials or include the full names of students in the credits of any published school produced video. Images of pupils will not be uploaded to generative AI tools or used to create AI generated content.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or school.

Parents may take photographs or videos of their own children at school events for personal use only. They are asked not to share images that include other children on social media.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the

school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Staff will adhere to the Pele Trust Social Networking Policy.

When official school social media accounts are established there should be:

- A process for approving members of staff to manage social media accounts
- At least two members of staff to monitor the accounts
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates

itself with the school or impacts on the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form. This does not apply to any image that may be an indecent image of a child, including an AI generated image, which must never be viewed, copied, screenshotted or printed.

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - the creation or sharing of AI generated sexual images of children
    - other criminal conduct, activity or materials

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Related policies and procedures:
This policy statement should be read alongside our organisational policies and procedures, including:

- Child Protection Policy
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Behaviour Policy
- Relationships and Health Education (RHE) Policy
- Pele Trust Social Networking Policy
- Staff disciplinary procedures
- Data protection and handling

Richard Coates
CE Primary School

Acceptable Use Agreement: Staff, Governors and Visitors

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr. James Watson, Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I understand that, if a personal mobile device is used to access my school email account, it is my responsibility to ensure that the account cannot be accessed by other users of the device. School email accounts will always be logged out of when not in use.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted. If an email attachment is opened on a personal device and contains personal information, it must not be saved on that device.
- I will not install any hardware or software without permission of the ICT Technician.
- I will only use generative AI tools that have been approved by the school. I will not enter personal or sensitive information about pupils, families or staff into any AI tool unless it has been approved for that purpose, and I will check AI generated content for accuracy before using it.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will report any filtering or monitoring concern, or any harmful content I see on a school device, to the DSL straight away.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- Images will not be stored on personal mobile devices and should only be taken on school devices.
- I will support our phone free school by not using my personal phone for personal reasons in front of pupils.
- I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment and that if I deliberately breach this agreement, disciplinary action may be taken and police contacted if necessary.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ..... Date .....

Full Name .....(printed)

Job title . . . . . .

Richard Coates CE Primary School

Monitoring and review

This policy and its implementation will be reviewed annually.

Review Date	Changes made	By whom	Ratification Date by Governing Body
April 2025	Review of policy with updates to sections on filtering and monitoring, pupil use of mobile phone devices on school premises and inclusion of Acceptable Use Agreement	James Watson	
October 2026	Updated in line with KCSIE 2026: four Cs updated to include AI; new section on artificial intelligence; deputy DSLs named; annual online safety review; filtering and monitoring review, testing and record keeping strengthened in line with DfE standards; phone free school day in line with statutory mobile phones guidance including smart glasses and connected devices; RHE 2025 guidance; parent engagement and AUP updated.	James Watson	

Belsay Primary School

Darras Hall Primary School

Heddon St. Andrew's CE Primary School

Ponteland High School

Ponteland Primary School

Richard Coates CE Primary School