Believe Grow Achieve

Copmanthorpe Primary School

Online Safety Policy

Approved by:	FGB	**Date:** September 2026
Last reviewed:	September 2025	
Next review due by:	September 2027	

Contents

1. Purpose and aims 3
2. Statutory framework and guidance 3
3. Understanding online safety risks 3
4. Roles and responsibilities 4
4.1 Governing Body 4
4.2 Headteacher and Designated Safeguarding Lead 4
4.3 ICT support provider 4
4.4 All staff, volunteers and contractors 4
4.5 Pupils 4
4.6 Parents and carers 4
5. Filtering and monitoring 5
6. Cybersecurity and school systems 5
7. Teaching online safety 5
8. Generative artificial intelligence (AI) 5
9. Mobile phones, personal devices and wearable technology 6
10. Responding to online safety concerns 6
11. Online bullying and child-on-child abuse 6
12. Sharing nudes and semi-nudes and harmful imagery 7
13. Staff use of technology, email and social media 7
14. Photography, video and publication 7
15. Working with parents and carers 8
16. Training 8
17. Monitoring and review 8
18. Links with other policies 8

.

1. Purpose and aims

1.1 This policy sets out Copmanthorpe Primary School's approach to keeping pupils, staff and the wider school community safe when using technology and online services.

1.2 Online safety is an integral part of safeguarding and child protection. The school recognises that technology can provide significant benefits for teaching, learning, communication and inclusion, while also creating risks which must be understood and managed.

1.3 The school aims to:

- provide a safe digital environment while enabling appropriate access to technology for learning
- help pupils develop the knowledge, skills and judgement to use technology safely, responsibly and respectfully
- identify pupils who may be at increased risk of online harm and provide appropriate support
- ensure staff understand their responsibilities for online safeguarding, filtering and monitoring
- respond promptly and proportionately to online safety concerns and safeguarding incidents
- work with parents and carers to promote safe and responsible use of technology.

2. Statutory framework and guidance

2.1 This policy has regard to current Department for Education (DfE) statutory and non-statutory guidance, including:

- Keeping Children Safe in Education (KCSIE) 2026
- the DfE filtering and monitoring core standard
- Teaching online safety in schools
- Searching, screening and confiscation at school
- Relationships Education, Relationships and Sex Education (RSE) and Health Education guidance
- Prevent duty guidance and guidance on protecting children from radicalisation
- DfE data protection guidance for schools, including guidance on generative artificial intelligence (AI)
- UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes.

2.2 The policy also has regard to relevant legislation, including the Education Acts, the Equality Act 2010, UK GDPR and the Data Protection Act 2018.

2.3 Where national guidance or legislation is updated, the school will apply the current requirements even where this policy has not yet been formally revised.

3. Understanding online safety risks

3.1 The school considers online safety through the four broad areas of risk identified in KCSIE:

Content – being exposed to illegal, inappropriate or harmful material, including sexual content, pornography, racism, misogyny, self-harm, suicide, misinformation, disinformation, radicalisation and extremism.

Contact – harmful interaction with other users, including peer pressure, grooming, exploitation, coercion, scams and adults posing as children.

Conduct – online behaviour which causes or increases the likelihood of harm, including bullying, sexual harassment, sharing nudes or semi-nudes, abusive communications, impersonation and misuse of personal information.

Commerce – risks including gambling, inappropriate advertising, phishing, financial scams and other attempts to exploit children financially.

3.2 The school recognises emerging and evolving risks, including generative AI, deepfakes and synthetic media, sextortion, harmful algorithms, persuasive design, online fraud and increasingly sophisticated manipulation of images, audio and video.

3.3 Online safety teaching and safeguarding responses will take account of pupils' age, developmental stage, communication needs and additional vulnerabilities. Some pupils, including pupils with SEND, may require more explicit, repeated or personalised teaching and support.

4. Roles and responsibilities

4.1 Governing Body

The Governing Body has overall responsibility for ensuring appropriate online safeguarding arrangements are in place. It will:

- hold the Headteacher to account for implementation of this policy
- ensure appropriate filtering and monitoring systems are in place and review their effectiveness at least annually
- ensure roles and responsibilities for filtering and monitoring are clearly assigned
- receive appropriate assurance and information about online safety, filtering and monitoring
- ensure staff receive appropriate safeguarding and online safety training
- ensure online safety remains an integral part of the school's wider safeguarding arrangements.

4.2 Headteacher and Designated Safeguarding Lead

The Headteacher is responsible for ensuring this policy is implemented consistently. The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety as part of the school's safeguarding arrangements and will:

- maintain an understanding of the filtering and monitoring systems and processes used by the school
- work with the school's ICT support provider and relevant staff to ensure systems remain appropriate and effective
- ensure online safety concerns are recorded, assessed and responded to through the school's safeguarding procedures
- ensure safeguarding alerts arising from monitoring are reviewed and acted upon appropriately
- liaise with children's social care, the police and other agencies where necessary
- provide governors with appropriate information about online safety and filtering and monitoring
- ensure staff receive regular safeguarding updates which include online safety.

4.3 ICT support provider

The school's ICT support provider, currently Vital, is responsible for the technical implementation and maintenance of agreed security, filtering and monitoring arrangements. This includes maintaining secure systems, applying updates and security controls, supporting appropriate filtering and monitoring and reporting significant technical concerns or failures to the school.

4.4 All staff, volunteers and contractors

All staff, volunteers and contractors must:

- understand and follow this policy and the relevant Acceptable Use Agreement
- recognise that online safety is a safeguarding responsibility
- use individual staff credentials appropriately and never attempt to bypass filtering, monitoring or security controls
- report filtering or monitoring failures, inappropriate access or online safety concerns promptly to the DSL or Headteacher
- record concerns on CPOMS where an individual child is involved, in line with safeguarding procedures
- respond professionally to disclosures and maintain an attitude that online abuse can happen here
- protect confidential and personal information when using technology.

4.5 Pupils

Pupils are expected to use school technology safely, respectfully and responsibly and to follow the school's Pupil Acceptable Use Expectations (Appendix 2). These expectations will be introduced and revisited at the start of each academic year and reinforced throughout the year. Pupils will be taught to seek help from a trusted adult when something online worries, upsets or confuses them.

4.6 Parents and carers

Parents and carers are encouraged to support the school's online safety expectations, discuss safe technology use with their children and raise concerns promptly with school.

5. Filtering and monitoring

5.1 The school uses Smoothwall filtering and monitoring systems to help protect pupils from harmful and inappropriate online content and to identify safeguarding concerns.

5.2 Filtering and monitoring form part of the school's safeguarding arrangements. They do not replace effective supervision, professional judgement, curriculum teaching or appropriate behaviour expectations.

5.3 The school will ensure that:

- harmful and inappropriate content is blocked without unreasonably restricting teaching and learning
- monitoring strategies are appropriate to the school's safeguarding needs
- the DSL and relevant staff understand how concerns and alerts are identified and escalated
- the effectiveness of filtering and monitoring is reviewed at least annually and following significant changes or incidents
- staff know how to report a concern, failure or suspected bypass of the systems
- staff and pupils do not attempt to disable or circumvent filtering or monitoring.

5.4 Filtering and monitoring arrangements will be considered in the context of the school's pupils, curriculum, SEND profile, devices, network and safeguarding risks.

6. Cybersecurity and school systems

6.1 The school will maintain proportionate technical and organisational measures to protect its systems, information and users from cyber threats.

6.2 Staff must follow the school's current cybersecurity and data protection arrangements, including requirements relating to passwords, multi-factor authentication where provided, software updates, device security, phishing and secure storage of information.

6.3 Staff must not install unauthorised software or connect unauthorised hardware to school systems. Suspected phishing, malware, data breaches or compromised accounts must be reported promptly.

6.4 School devices must be secured when unattended. Work devices taken off site must be used and stored in a way that protects school information and prevents unauthorised access.

6.5 Personal devices must not be used to store or process school information unless explicitly authorised and appropriate safeguards are in place.

7. Teaching online safety

7.1 Online safety will be taught through the curriculum, including Computing, Relationships Education and Health Education, and reinforced across other subjects where appropriate.

7.2 Teaching will be age appropriate and will include:

- safe and respectful use of technology
- privacy, personal information and passwords
- recognising harmful, inappropriate or misleading content
- healthy online relationships and respectful communication
- online bullying, coercion and harmful behaviour
- how information, images and data can be copied, altered and shared
- recognising scams, manipulation and attempts to exploit trust
- how to report concerns and seek help
- critical thinking about online information, including AI-generated and manipulated content.

7.3 Teaching will be adapted where necessary for pupils with SEND or other vulnerabilities and will take account of pupils' lived online experiences without assuming that all pupils have the same access, understanding or level of risk.

8. Generative artificial intelligence (AI)

8.1 The school recognises that generative AI is an increasingly common technology which can provide educational and administrative benefits when used safely, appropriately and professionally.

8.2 The school will take a proportionate approach to AI and will consider safeguarding, data protection, intellectual property, accuracy, bias, age restrictions and the educational purpose of any proposed use.

8.3 Staff may use approved generative AI tools to support professional work where this is consistent with school expectations and data protection requirements. AI-generated material must be checked carefully for accuracy, appropriateness and bias. Professional responsibility for material ultimately used or shared remains with the member of staff.

8.4 Staff must not enter identifiable, special category or confidential information about pupils, families, staff or other members of the school community into generative AI systems unless the particular system and use have been explicitly approved for processing that information.

8.5 Pupils will only use generative AI in school where this has been specifically authorised and appropriately supervised by staff. The school will have regard to the age requirements and safety features of individual services.

8.6 Pupils will be taught, at an age-appropriate level, that AI-generated information may be inaccurate or misleading and that images, audio and video can be manipulated or artificially generated.

8.7 AI must not be used to create, manipulate or distribute harmful, abusive, sexualised, discriminatory or deceptive content, including deepfakes or material intended to impersonate another person.

9. Mobile phones, personal devices and wearable technology

9.1 Pupils may only bring mobile phones or personal electronic devices to school in accordance with the school's Mobile Phone Policy and any permission arrangements in force.

9.2 Where a pupil is permitted to bring a device to school, it must be handed in or stored as required by the Mobile Phone Policy and must not be used during the school day unless specifically authorised.

9.3 Smart watches and other connected or recording devices are subject to the same principles. The school may restrict their use where features such as messaging, photography, audio recording or internet access create safeguarding, privacy or learning concerns.

9.4 Staff use of personal devices must comply with the Staff Code of Conduct and the staff Acceptable Use Agreement.

10. Responding to online safety concerns

10.1 Online safety concerns involving a child will be treated as safeguarding concerns and responded to in accordance with the Child Protection and Safeguarding Policy.

10.2 Staff should not investigate safeguarding concerns themselves beyond what is necessary to establish the basic facts and ensure immediate safety. Concerns must be passed promptly to the DSL or a deputy.

10.3 The DSL will consider the nature and seriousness of the concern, the children involved, any immediate risk, whether parents should be informed and whether referral to children's social care, police or another agency is required.

10.4 Online safety incidents will be recorded appropriately. Where a child is involved, CPOMS will normally be used in accordance with the school's safeguarding recording procedures.

10.5 Where misuse does not constitute a safeguarding concern, the school may respond through the Behaviour Policy, Staff Code of Conduct, disciplinary procedures or other relevant policy.

10.6 Searching, confiscation and examination of electronic devices will be undertaken only in accordance with current DfE guidance, the Behaviour Policy and safeguarding procedures.

11. Online bullying and child-on-child abuse

11.1 Online bullying is behaviour carried out through digital technology which causes harm. It may include messages, images, videos, impersonation, exclusion, harassment or repeated unwanted contact.

11.2 The school recognises that online behaviour can form part of child-on-child abuse, including sexual harassment, coercive behaviour, misogynistic abuse, discriminatory abuse and sharing sexual imagery.

11.3 Reports will be taken seriously, recorded and responded to in a way that safeguards the child who has experienced harm and considers the needs and behaviour of the child responsible.

11.4 The school will consider the relationship between online and offline behaviour and may respond to online incidents occurring outside school where they affect safeguarding, pupils' wellbeing or the safe and orderly running of the school.

12. Sharing nudes and semi-nudes and harmful imagery

12.1 Any incident involving the sharing of nudes or semi-nudes by children will be treated as a safeguarding matter and managed in accordance with current UKCIS guidance.

12.2 If such an incident comes to the attention of a member of staff, they must report it to the DSL immediately.

12.3 Staff must not view, copy, print, share, store or save the imagery, ask a child to share or download it, or ask the child to delete it. If imagery has been viewed accidentally, this must be reported to the DSL.

12.4 Staff should reassure the child that they have done the right thing by speaking to an adult, should not blame or shame them and should explain that the concern needs to be passed to the DSL.

12.5 The DSL will undertake the necessary review and risk assessment, including consideration of coercion, exploitation, adult involvement, malicious sharing, the child's age and understanding, SEND or other vulnerabilities and whether other agencies need to be involved.

12.6 Only in exceptional circumstances may the DSL decide that viewing imagery is necessary to safeguard a child. Any such decision will be based on professional judgement and current UKCIS guidance.

12.7 Where an adult is suspected of sharing sexual imagery involving a child, or there is evidence of adult involvement in child sexual abuse, the matter will be referred urgently in accordance with safeguarding procedures.

13. Staff use of technology, email and social media

13.1 Staff must maintain professional boundaries when using technology and must comply with the Staff Code of Conduct, data protection requirements and the staff Acceptable Use Agreement.

13.2 School systems and accounts should be used for school business. Staff must not use personal social media or messaging accounts to communicate privately with pupils.

13.3 Confidential information about pupils, families, colleagues or school business must not be published or discussed through personal social media or other unauthorised platforms.

13.4 Staff must consider privacy and professional reputation when using social media personally and must not post content which compromises safeguarding, confidentiality, professional boundaries or confidence in the school.

13.5 Staff must not use personal devices to photograph or record pupils except where explicitly authorised for a specific school purpose. School-provided devices should normally be used.

14. Photography, video and publication

14.1
The school may take photographs or video of pupils for educational, assessment, celebration, communication and publicity purposes where there is an appropriate lawful basis. Images will be used in accordance with the school's privacy information, safeguarding procedures and parental permissions where these are required.

14.2
The school collects and reviews parent/carer preferences regarding the use and publication of pupil photographs and video through its annual permissions process. Parents and carers may change their preferences at any time by contacting the school.

14.3
Before publishing or sharing identifiable images externally, staff must check the pupil's current recorded permissions and consider whether there are any additional safeguarding, privacy or welfare concerns. Permission to use an image does not remove the need for staff to make an appropriate professional judgement about whether publication is suitable.

14.4
The school will avoid unnecessary identification of pupils. Personal information will not normally be published alongside an identifiable image unless there is a clear reason for doing so and the appropriate permission is in place.

14.5
Images and recordings must be appropriate, respectful and stored securely. Staff must use school-authorised

devices, accounts and systems when taking, storing or sharing images of pupils and must not routinely use personal devices for this purpose.

14.6
Parents and carers may take photographs or recordings at school events where the school has permitted this. These should be for personal or family use and families are asked to respect the privacy of other children and not publicly share identifiable images or recordings of other pupils without appropriate permission. The school may restrict photography or recording at particular events where there are safeguarding, privacy or welfare concerns.

14.7
Where a child's individual safeguarding circumstances mean that photography, recording or publication may present an increased risk, specific arrangements will be put in place and communicated to relevant staff. These arrangements take precedence over general permissions recorded by the school.

15. Working with parents and carers

15.1 The school will provide parents and carers with information about online safety and will encourage an open partnership around children's use of technology.

15.2 The school will communicate relevant information about filtering and monitoring, age-appropriate online safety education and significant changes to the technology pupils are expected to use.

15.3 Parents and carers should raise concerns with the school where online behaviour is affecting a child's safety, wellbeing or education, even where the behaviour has occurred outside school.

15.4 The school may signpost families to reputable national sources of advice and reporting routes, including CEOP, Childnet, the UK Safer Internet Centre, Internet Watch Foundation and NSPCC.

16. Training

16.1 New staff will receive online safety information as part of safeguarding induction.

16.2 All staff will receive online safety training as part of safeguarding training and regular updates as required. Training will include staff responsibilities for filtering and monitoring.

16.3 The DSL and deputies will maintain appropriate knowledge of current online safeguarding risks and guidance.

16.4 Governors will receive appropriate safeguarding training which includes online safety and their responsibilities for filtering and monitoring.

16.5 Additional training will be provided where incidents, technological changes or identified risks indicate that this is necessary.

17. Monitoring and review

17.1 The DSL will maintain oversight of online safety concerns and use safeguarding information to identify themes, emerging risks and areas requiring further action or education.

17.2 Filtering and monitoring arrangements will be reviewed at least annually and following significant incidents, changes to systems or material changes in risk.

17.3 This policy will be reviewed annually by the Headteacher/DSL with appropriate input from the Computing Lead, ICT support provider and governors.

17.4 Because technology and online harms change rapidly, operational procedures may be updated between formal policy reviews where necessary to maintain effective safeguarding.

18. Links with other policies

This policy should be read alongside the school's:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Mobile Phone Policy
- Data Protection Policy and privacy notices
- Computing curriculum documentation

- Complaints Procedure
- Capability and disciplinary procedures where relevant.

Appendix 1 – Acceptable Use Agreement for Staff, Governors, Volunteers and Other Adults

Access to the school's technology, systems, network and information carries a responsibility to use them safely, securely and professionally. This agreement should be read alongside the Online Safety Policy, Staff Code of Conduct and Data Protection Policy.
By accessing school systems, I understand and agree that I will:

- use school technology, accounts and systems appropriately and only for authorised purposes connected with my role
- keep passwords and authentication details secure and use only my own account
- protect confidential and personal information and use only approved systems for storing, accessing or sharing it
- follow the school's cybersecurity, data protection, filtering and monitoring arrangements
- never attempt to bypass or disable filtering, monitoring, security or device-management controls
- report suspected phishing, compromised accounts, data breaches, security incidents or failures in filtering and monitoring promptly
- maintain appropriate professional boundaries in all online communication
- not use personal social media or messaging accounts to communicate privately with pupils
- use school-authorised devices and systems when photographing, recording or storing images of pupils, unless an alternative has been specifically authorised
- check relevant permissions and safeguarding considerations before publishing or sharing photographs, video or other information about pupils
- only use generative AI in accordance with school expectations and never enter identifiable, sensitive or confidential school information into an AI system unless that particular use has been approved
- report any online safeguarding concern involving a child immediately in accordance with the school's safeguarding procedures
- ensure that pupils in my care use technology safely and appropriately.
-

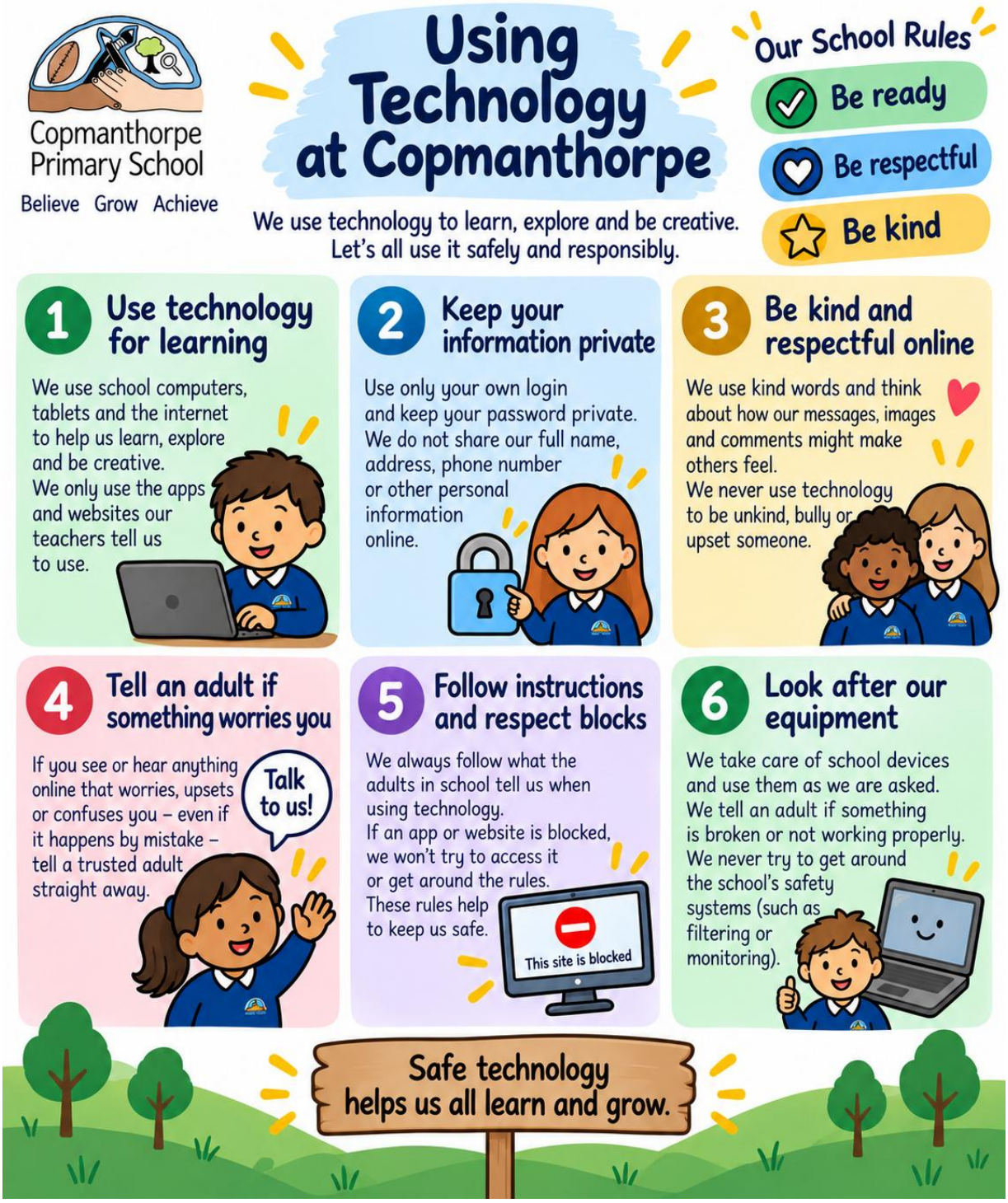
Safeguarding imagery
If I become aware of suspected nude or semi-nude imagery involving a child, I will **not view, copy, print, share, store or save the imagery**, ask a child to share or download it, or ask them to delete it. I will report the concern immediately to the DSL.

Professional responsibility
I understand that use of school systems may be filtered and monitored for safeguarding, security and appropriate-use purposes.
I will not use school technology in a way that is unlawful, compromises safeguarding or security, breaches confidentiality or could reasonably undermine professional standards or confidence in the school.

Name:
Role:
Signature:
Date:

Appendix 2 – Pupil Acceptable Use Expectations

The poster below sets out the school's acceptable use expectations for pupils in a clear and age-appropriate way. These expectations apply to all pupils when using school technology, devices and online services and form part of the school's normal expectations for behaviour rather than requiring a separate signed agreement.

The expectations will be introduced and revisited with all pupils at the start of each academic year and regularly reinforced through Computing and online safety teaching, assemblies and day-to-day use of technology. Staff will also revisit them during the year where appropriate, including in response to emerging issues or concerns.

The expectations are underpinned by the school rules of Be Ready, Be Respectful and Be Kind and should be displayed or readily available in classrooms where technology is used.