Bradford Diocesan Academies Trust

Clayton St John ONLINE SAFETY POLICY

AWAITING APPROVAL 13/10/26 LGB MEETING

CLAYTON ST JOHN
C of E PRIMARY SCHOOL

Reviewed: September 2026
Next Review Due: September 2027

Bradford Diocesan Academies Trust

Table of Contents

Item	Page
1. Trust Policy Statement	3
2. Introduction and Aims	3
3. Key Staff	5
4. Online Safety Trends	5
5. Roles and Responsibilities a. Local Governing Body b. Headteacher c. Designated Safeguarding Lead d. IT Staff e. All Staff and Volunteers f. Curriculum Leaders g. Parents h. Pupils g. Visitors and Members of the Community	7
6. Educating Pupils about Online Safety	12
7. Raising Awareness with Parents and Carers about Online Safety	13
8. Key Online Safety Issues a. Cyber Bullying b. Sexual Violence and Harassment c. Nude and Semi-Nude Images including where Generated by Artificial Intelligence d. Online Extremism and Radicalisation e. Social Media	14
9. Searching and Screening Procedures	17
10. Acceptable Use of the Internet in School Pupils Using Mobile Devices in School	18
11. Staff Using School Devices Outside Work	19
12. Responding to Issues of Misuse	19
13. IT Systems and Access	20
14. Filtering and Monitoring a. Filtering b. Monitoring	21
15. Using the Internet and Email	21
16. Use of Generative Artificial Intelligence	22
17. Publishing Content Online	23
18. Training	23
19. Policy Monitoring Arrangements	24
20. Links to Guidance and Other Policies	25
Appendix One: Summary of Policy Changes	26

APPROVAL 13/10/26 LGB MEETING

1. Trust Policy Statement

Bradford Diocesan Academies Trust (BDAT) regards knowing how to stay safe online as integral to the development and safeguarding of our pupils. We are committed to developing a culture where pupils are aware of the risks they face online and know how to keep themselves safe, but where they can also harness the opportunities within the digital world to enhance their education.

We aim to ensure our schools:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile technology, smart technology and generative artificial intelligence tools
- Establish clear mechanisms to identify, intervene and escalate any online safety incidents including using filtering and monitoring systems on all school devices

As part of our focus on diversity and inclusion, BDAT pledges that our policies will seek to promote equality, fairness, and respect for all staff and pupils. Our policies reflect the BDAT values of inclusion, compassion, aspiration, resilience, and excellence. By working closely with a range of stakeholders, such as our school, union, and HR colleagues, we have ensured that BDAT's policies do not unlawfully discriminate against anybody.

This policy should be read in conjunction with our school specific Behaviour Policy, Safeguarding and Child Protection Policy and Anti-Bullying Policy, along with other Trust level policies held on the BDAT website. It will be reviewed annually in order to assess its implementation and effectiveness.

For the purpose of this policy, the term Trust refers to BDAT. The term school and the term academy are interchangeable. The term pupil and the term student are interchangeable.

AWAITING APPROVAL 15/10/25 JOB MEETING

2. Introduction and Policy Aims

Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support teaching and learning, as well as playing an important role in the everyday lives of children, young people and adults. New technologies have become integral in today's society, both within schools and outside schools.

The internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should always have an entitlement to safe internet access and, consequently, schools need to build in the use of these technologies to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society, exemplified by the rapid development of generative artificial intelligence tools such as Chat GPT. Currently the internet technologies staff, children and young people are using include:

- Websites
- E-mail, instant messaging and chat rooms
- Social Media (including Facebook, X, Snapchat, Instagram, TikTok, WhatsApp, Discord)
- Mobile phones with text, video and/or web functionality
- Making/receiving phone calls via their mobile phones
- Other mobile devices with web functionality such as Smartwatches
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting and Live Streaming
- Music Downloading
- Generative Artificial Intelligence programmes

This policy recognises the commitment of Clayton St John to online safety and acknowledges its part in our overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

We know about the benefits of rationing time spent online for children, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.

We pay due regard to DFE Guidance on Mobile Phones in Schools and our school is a mobile phone free environment by default.

We also believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The online safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

Keeping Children Safe in Education 2026 references four areas of risk online within part two, these being:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated by AI and online bullying

AWAITING APPROVAL 13/10/26 LGB MEETING

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through strong educational provision that we build our pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. This involves all stakeholders.

3. Key Staff

KCSIE makes clear that the Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). The DSL can delegate activities but not the responsibility for this area and whilst subject leads (e.g. for RSHE) will plan the curriculum for their area, it is important that this ties into a whole-school approach.

The below table details the staff and governors with specific responsibilities relating to online safety:

Role	Name
Designated Safeguarding Lead (Overall Responsibility for Filtering and Monitoring)	Mrs Emsley
Deputy Designated Safeguarding Lead	Mrs Allingham
Safeguarding Team/Other Named Persons	Miss Hughes
Nominated Governor for Safeguarding	Mr Verma
Curriculum Leads with Relevance to Online Safety	Mrs Miller -Computing Lead Miss Hopkins -PSHE Lead

AWAITING APPROVAL 15/10 - LGB MEETING

4. Online Safety Trends

In our school over the past year, we have particularly noticed the following in terms of types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Online bullying via social media groups such as what's app at home.
- Typing into search engines inappropriate searches.

At Clayton St John, we are mindful that the online world is ever developing, and we recognise that we must be vigilant in being aware of and responding to new risks that may harm our pupils.

For example, the increasing prevalence of generative artificial intelligence (AI) remains an exponentially growing concern, with pupils potentially having access to tools that generate text, images and videos at home or in school.

Thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI "girlfriends," unregulated therapy bots, and even chatbots that encourage self-harm or suicide—tools many students can access freely at home or school.

Chatbots can also blur reality, offer harmful advice or engage in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation. Tragically, there have been numerous cases worldwide of children dying by suicide as a result of interactions with such bots.

When used for generating text, generative AI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content. Sometimes they can be used to generate hoaxes and disinformation which is so realistic that it is difficult to determine what is real and what is not.

Beyond text, generative AI makes it easier than ever to create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. The Internet Watch Foundation has warned of a sharp rise in AI-generated child sexual abuse imagery.

Alarming reports also show children using nudifying apps to create illegal content of peers. It's critical to stress that in the UK, any CSAM (child sexual abuse material)—AI-generated, photographic, or even cartoon—is illegal to create, possess, or share.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2026' has shown that Internet use is nearly universal, with 99% of 8-17-year-olds going online, and the vast majority of children are using digital technology by the time they start primary school. A critical transition occurs at age 11, where personal mobile phone ownership jumps from 56% to 83%.

Schools must also address the rapid adoption of Generative AI, now used by 56% of 8-17-year-olds, primarily for schoolwork (51%). Despite high confidence, a 'digital literacy gap' exists: 31% of students could not identify a fake social media profile, and 46% believe AI search summaries are "always accurate".

Social pressures remain high, with 70% of students feeling pressure to be popular on social media apps. Negative experiences are common; 23% of 8–17-year-olds personally experienced "nasty or hurtful" behaviour in the last year, occurring most frequently on social media (47%) and in online games (38%). Vulnerable students, such as those with mental health conditions, are significantly more likely to feel their screen time is "too high" (56%).

Schools are the primary source of online safety information for 49% of parents. While 85% of students recall online safety lessons, only 23% remember being taught how to spot AI-generated content, and 21% recall lessons on identifying advertising.

As a school we recognise that many of our children and young people are using social media apps and online games regardless of age limits, which are often misunderstood, ignored or bypassed, particularly as it can often be the case that children are more technologically literate than many adults.

Growing numbers of children and young people are using social media and apps, primarily TikTok as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news.

The Revealing Reality: Anti-Social Media Report 2023 highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons.

AWAITING APPROVAL 13/10/26 LGB MEETING

At the same time, the Children's Commissioner Report 'A lot of it is actually just abuse' revealed the ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys across the world over the past year.

Data from the Internet Watch Foundation (IWF) in their 2025 annual report highlights the scale of child sexual abuse imagery online. In 2025, the IWF assessed 451,210 reports, confirming that 311,610 contained child sexual abuse material (CSAM).

Emerging and persistent harms identified by the IWF include:

- Sexually coerced extortion (sextortion): Targeted threats against students – teenage boys in particular.
- AI-generated abuse: The use of generative tools to create non-consensual sexual imagery.
- Violence against women and girls (VAWG): A growing trend in digital spaces around violent and misogynistic narratives and language.

A further concern highlighted by the National Crime Agency, is that of the existence of 'Com Networks'. These are networks of predominantly teenage boys, dedicated to inflicting harm and committing a range of criminality both on and offline, including cyber, fraud, extremism, serious violence, and child sexual abuse.

The victims of these crimes are typically other children, some as young as 11, who have been coerced into seriously harming or sexually abusing themselves, siblings or pets. These networks are not hidden away in the dark web, but instead on platforms such as Discord, Telegram, Roblox, and Minecraft.

Cyber Security also remains an essential component in safeguarding children. Data from the Department for Science, Innovation and Technology (DSIT) states that 73% of secondary schools and 49% of primary schools identified a cyber breach or attack in the past 12 months (a significant jump from the previous year).

Phishing remains the biggest entry point and AI is being used by scammers to generate sophisticated, error-free phishing emails targeting school administration and staff accounts.

AWAITING APPROVAL 15/10/26 LGB MEETING

5. Role and Responsibilities

In the landscape of the challenges outlined above, it is vital that all stakeholders work together to ensure that our pupils remain safe in the online world. This section outlines the roles and responsibilities of the various stakeholders.

5.1 The Local Governing Body

The governing body has overall responsibility for monitoring this policy, holding the Headteacher to account for its implementation and reviewing its effectiveness.

The governing body will ensure that online safety is a focus of its safeguarding quality assurance activities. In particular, the nominated safeguarding governor will monitor the online safety arrangements through regular meetings with the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while monitoring the whole school approach to safeguarding (e.g. by asking questions such as those from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board)
- Support the work of Clayton St John in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in online safety awareness
- Have an overview of how the school IT infrastructure provides safe access to the internet through its filtering and monitoring systems and the steps Clayton St John takes to protect personal and sensitive data.
- Ensure appropriate funding and resources are available for Clayton St John to implement their online safety strategy
- Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum.

5.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout Clayton St John. They will:

- Liaise with the Governors to ensure they are provided with relevant online safety information
- Develop and promote an online safety culture within the school community and whole-school safeguarding approach
- Ensure that all staff and governors receive suitable CPD to enable them to carry out their roles in relation to online safety
- Ensure that all staff, pupils and other users agree to the ICT Acceptable Use Policy and that new staff have online safety included as part of their induction procedures
- Receive and regularly review online safety incident logs through their line management of the Designated Safeguarding Lead; ensuring that the correct procedures are followed should an online safety incident occur in school and review incidents to see if further action is required
- Ensure the school implements and makes effective use of appropriate ICT systems and services including filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a compliant framework for storing data but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.

5.3 The Designated Safeguarding Lead (DSL)

The details of our DSL and deputies are set out in this policy as well as in the Safeguarding and Child Protection Policy and their relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

AWAITING APPROVAL 13/10/20 LGB MEETING

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout Clayton St John.
- Working with the Headteacher, IT staff and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Clayton St John Safeguarding and Child Protection Policy, including making referrals to external agencies such as Children's Social Care, the Police and the Local Authority Designated Officer as necessary.
- Ensuring that any online safety incidents, including those related to filtering and monitoring, are logged on CPOMS and dealt with appropriately in line with this policy
- Receive regular updates about online safety issues and legislation, be aware of local and school trends
- Work with IT staff to ensure that filtering and monitoring systems are appropriately setup to prevent both under and over-blocking
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Anti-Bullying Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and Local Governing Body
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents

5.4 IT Staff

The BDAT Head of Corporate Projects is responsible for managing and overseeing the Trust-wide ICT Managed Service Provision, whose responsibilities include the following:

- Collaborating regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online whilst at school, including terrorist and extremist material
- Ensuring that Clayton St John's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting security checks and monitoring our ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Supporting Clayton St John in providing a safe technical infrastructure to support teaching and learning
- Ensuring appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information and reviewing these regularly to ensure they are up to date
- Ensuring that provision exists for misuse and malicious attack detection
- Ensuring that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems by administrative staff, including password management

AWAITING APPROVAL 13/10/26 LGB MEETING

- Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.
- Ensuring that suitable access arrangements are in place for any external users of our ICT equipment
- Ensuring appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

5.5 All Staff and Volunteers

All staff and volunteers at Clayton St John are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Reporting any unblocked websites that could be harmful to the DSL
- Informing the DSL if they are teaching any topics that could lead to an influx of filtering and monitoring alerts
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with our Anti-bullying Policy
- Taking responsibility for ensuring the safety of sensitive school data and information
- Developing and maintaining an awareness of current online safety issues, legislation and guidance relevant to their work
- Always maintaining a professional level of conduct in their personal use of technology
- Ensuring that all digital communication with pupils is on a professional level and only through school-based systems, NEVER through personal email, text, mobile phone social network or other online medium.
- Embedding online safety messages in learning activities where appropriate
- Supervising pupils carefully when engaged in learning activities involving technology
- Ensuring that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable

5.6 Curriculum Leaders

Teaching pupils about online safety is a fundamental part of the whole-school approach in this area. All subject leaders should seek opportunities to embed online safety in their subject. The PSHE/RSHE Lead and the Computing Lead will play a particularly important role.

The PSHE/RSHE Lead will:

- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing nude or semi-nude pictures online into the curriculum. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.

AWAITING APPROVAL 13/10/26 LGB MEETING

- Focus on the underpinning knowledge and behaviours outlined in Teaching Online Safety in Schools in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE/RSHE, adapting the curriculum to respond to any patterns and trends in online safety safeguarding issues.

The Computing/ICT Lead will:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing, adapting the curriculum to respond to any patterns and trends in online safety safeguarding issues.

5.7 Parents

Clayton ST John would ask that all our parents and carers support the aims of this policy by:

- Ensuring their child (where age appropriate) has read, understood and agreed to our terms on acceptable use of ICT systems and internet
- Helping and supporting the school in promoting online safety with their children
- Discussing online safety concerns with their children, showing an interest in how they are using technology, and encouraging them to behave safely and responsibly when using technology
- Consulting with Clayton St John if they have any concerns about their child's use of technology
- Supporting our approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

5.8 Pupils

All pupils at Clayton St John are expected to:

- Take responsibility for their own and each other's' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights and values of other pupils in their use of technology at school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all online safety incidents to appropriate members of staff in school
- Discuss online safety issues with family and friends in an open and honest way
- Know, understand and follow school policies on the use of technology to an age-appropriate level
- Know, understand and follow school policies regarding bullying to an age-appropriate level

AWAITING APPROVAL 13.10.26 LGB MEETING

- Support the Clayton St John approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

5.9 Visitors and Members of the Community

Visitors and members of the community who use Clayton St John's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

If visitors are concerned about the welfare of a pupil for any reason, they should report it to the DSL without delay.

6. Educating Pupils about Online Safety

Despite the risks associated with being online, Clayton St John recognises the opportunities and benefits to children too. Technology is a fundamental part of adult life and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

At Clayton St John, pupils will be taught about online safety through:

- An age-appropriate curriculum which has online safety related lessons embedded throughout, but with a planned online safety programme as part of the ICT/Computing and PSHE curricula which build knowledge and skills sequentially as pupils move through school.
- Staff will deliver lessons that challenge pupils, provide feedback on their progress and use assessment to identify where pupils may need extra support or intervention.
- Celebration and promotion of online safety through collective worship and whole-school activities, such as Safer Internet Day each year.

In the Early Years and Foundation Stage, there is specific guidance on the use of screen time within schools and we will ensure that our offer fully complies with it.

In Key Stage 1, pupils will be taught to:

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

AWAITING APPROVAL 19/03/26 GB MEETING

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly, keeping personal information private
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
  How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

We utilise data from our safeguarding reports, filtering logs, monitoring captures and other stakeholder feedback to inform our curriculum, so that we are constantly learning from concerns and being reflexive and responsive to the needs of our children.

We recognise that nationally, children with SEND are less likely to receive effective online safety teaching but are more at risk of being a victim of harm caused online. Therefore, we will ensure that we adapt our curriculum and teaching of online safety for all children, especially those with SEND. We will also consider whether specific filtering policies are required for particular children to afford more protection from online harms. We will also consider targeted and individual interventions that children need to protect them from harm and prevent future online harm.

AWAITING APPROVAL 13/10/26 LGB MEETING

7. Raising Awareness with Parents and Carers about Online Safety

Clayton St John will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. We will let parents know:

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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL or a member of the safeguarding team.

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

UK Safer Internet Centre - What are the Issues?
Childnet International - Hot Topics
Childnet International - Parent Factsheet
Online Safety Basics - National Cybersecurity Alliance
Parent Zone - Working Towards a Safer Digital World
TALK Checklist by the Internet Watch Foundation
LGfL - Generative AI Information for Parents
Keeping children safe online | NSPCC
Topic: Digital Wellbeing | SWGfL
Parents and Carers - UK Safer Internet Centre
Parent Guides from ConnectSafely - ConnectSafely
LGfL - Parent Safe Resources

8. Key Online Safety Issues

8.1 Cyber Bullying

Cyber bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group.

Cyber bullying includes sending abusive or hurtful texts, emails, social media posts, images or videos, deliberately excluding others online, spreading nasty gossip or rumours online, imitating others online or using their log-in or using generative AI to facilitate any of these behaviours.

Cyber bullying can be overt or covert but uses digital technologies, including hardware such as computers and smartphones, and software such as social media, instant messaging, texts, websites, generative AI applications and other online platforms. Cyber bullying can happen at any time, can be in public or in private online spaces and so is sometimes only known to the target and the person bullying.

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

Clayton St John will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

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

The DSL will consider whether the incident should be reported to the Police if it involves illegal material and will work with external services if it is deemed necessary to do so.

AWAITING APPROVAL 13/10/26 LGB MEETING

8.2 Sexual Violence and Harassment

Keeping Children Safe in Education is clear that sexual violence and harassment can take place online as well as physically in person. Any such incidents must be reported to the DSL who will lead on a safeguarding response.

All staff are responsible for fostering a zero-tolerance culture when it comes to sexual violence and harassment, never dismissing unacceptable behaviour as 'banter' and always maintaining an attitude that it could happen here.

Sexual violence includes causing someone to engage in sexual activity without consent, which could occur online. For example, someone being coerced on a video call to strip or touch themselves sexually.

Online sexual harassment could include the sending of unwanted sexualised comments or images, consensual and non-consensual sharing of nude or semi-nude images, sexualised jokes or sharing of explicit content.

Digital technology can also be used to facilitate sexual harassment in person. For example, 'upskirting' has become more prevalent due to the increased use of smart glasses and other discreet recording technology that can capture imagery without individuals knowing.

Our curriculum teaches pupils about healthy relationships (including those online) at an age-appropriate level. We ensure that all our pupils know what to do and who to report it to in the event that they experience any kind of sexual violence or harassment, either online or offline.

8.3 Nude and Semi-Nude Images

Where there is a disclosure from a pupil and/or we become aware that a child may have been involved in sharing 'nude or semi-nude' images, our schools will refer to the guidance in the UKCIS document 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

Images include all visual content such as photos, videos and livestreams. Images may be taken by the child themselves or taken or created by another person. They may also be digitally altered or wholly generated using artificial intelligence, including what are sometimes described as 'deepfakes' or 'deep nudes'.

Our staff understand that when the sharing of nude or semi-nude images comes to their attention:

- The incident must be referred to the DSL immediately
- The DSL should hold an initial review meeting with appropriate school staff
- There will be subsequent interviews with the young people involved (as appropriate)
- Parents will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- The DSL will assess the information available and with the use of appropriate risk assessment tools, decide the appropriate response by the school to such an incident. The Bradford Partnership Harmful Sexual Behaviour Protocols may be useful in this process.

AWAITING APPROVAL 13/10/26 LGB MEETING

- If at any point in the process it has been established a young person has been harmed or is at risk of harm, or such behaviour involves a young person communicating with an adult, then a referral will be made to Children's Social Care and/or the Police immediately

Staff should never intentionally view any nude or semi-nude images. This decision can only be taken by the DSL in exceptional circumstances where it is necessary to safeguard a child and will be done so in line with the DFE guidance linked above. The school may also make use of guidance from The Marie Collins Foundation with regards to supporting victims of Technology Assisted Child Sexual Abuse.

Everyone must understand that whilst the sharing of intimate or sexual images involving children (created via AI or otherwise) is illegal, pupils should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

AWAITING APPROVAL 13/10/26 LGB MEETING

8.4 Online Extremism and Radicalisation

The Counter-terrorism Local Profile and our Prevent Risk Assessment both indicate that the most likely way in which a pupil will be exposed to extremist material is online.

Misinformation, disinformation and conspiracy theories are all prevalent in the online world, with some platforms allowing any content to be posted without moderation. Algorithms on such platform mean that clicking one link (even unintentionally) can lead to a user being exposed to this type of content repeatedly.

This poses additional risks as increasing numbers of cases dealt with by the Police link to people who have become 'self-initiated' extremists by being exposed to this type of content, alongside those who are targeted by extremist groups.

Our curriculum aims to teach pupils about disinformation and so-called fake news, whilst empowering them with the critical thinking skills to analyse and verify information they see online.

8.5 Social Media

Social media incidents involving pupils can often be safeguarding concerns and may link to the other concerns outlined within this section.

We recognise that social media is a significant part of modern life for children and young people but strongly advocate that parents ensure their children are only accessing platforms in line with the recommended age limits, particularly in light of the government announcement of a forthcoming social media ban for under 16-year-olds.

We expect our pupils to use any social media platforms in line with the Behaviour Policy, Acceptable Use of ICT Agreement and our school values.

Where a social media post is inappropriate, offensive, upsetting or abusive we will request that the member of the school community who posted it removes it immediately, as well as following up via the relevant policy depending on who the poster is. The Police may be contacted if an offence has been committed.

Where an offensive post is made about a member of staff, we will report it to the platform it is hosted on and may contact the Professionals' Online Safety Helpline for further support.

9. Searching and Screening Procedures

The Headteacher, and any member of staff authorised to do so by them (such as the DSL, senior leaders and the pastoral team), can carry out a search of a pupil in line with DFE Guidance on Searching and Screening and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or Designated Safeguarding Lead.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or;
- Disrupt teaching, and/or;
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher, Designated Safeguarding Lead or another member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

AWAITING APPROVAL 17/10/26 LOB MEETING

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

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

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

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

AWAITING APPROVAL 13/11/26 LGB MEETING

10. Acceptable Use of the Internet in School

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Clayton St John's ICT systems and the internet. Visitors will also be expected to read and agree to terms of acceptable use if relevant.

Use of Clayton St John's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) through our filtering and monitoring systems to ensure they comply with the BDAT Acceptable Use of IT Policy.

Where pupils are provided with devices that they can use at home, their use is still covered by the IT Acceptable Use Policy, and the device will still be subject to the filtering and monitoring systems.

11. Pupils Using Mobile Devices in School

DfE Guidance on Mobile Phones in Schools is clear that schools should be mobile phone free environments by default. This means that pupils should not have access to their mobile phones whilst on school premises.

Clayton St John, our approach is only year 5 and 6 pupils may bring phones into school. They will be switched off and placed in a safe container during the day in a locked cupboard and returned at the end of the day.

Personal recording devices, such as smart glasses, are not permitted in school without written permission. It is forbidden to take secret photos, videos or recordings of teachers or pupils, including remotely, with any device.

For school trips/events away from school, teachers will be issued a school duty phone, and this number will be used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be reported immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure the number is hidden to avoid a parent or pupil accessing a teacher's private phone number.

Parents will be informed about their child's permitted device use whilst on trips away from school as part of the planning process for the trip.

12. Staff Using School Devices Outside Work

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

BDAT ensures that all laptops provided for use inside and outside school have:

- Anti-virus and anti-spyware software installed
- Up-to-date operating systems with the latest updates installed

Staff members must not use the device in any way which would violate the BDAT Acceptable Use of IT Policy. Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from a member of IT support.

13. Responding to Issues of Misuse

Where a pupil misuses the ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Acceptable Use of IT. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

Clayton St John will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the Police.

AWAITING APPROVAL 15/10/25 LGB MEETING

14. IT Systems and Access

In collaboration with our trust-wide IT Managed Service Partner, Clayton St John decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their role in school and will be responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Pupils are taught about safe practice in the use of their log in and passwords.

Staff are also given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

Our practice in relation to passwords is as follows:

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, CPOMS, school management information system). This may require two-factor authentication.
- We provide all staff with a unique, individually named user account and password for access to IT equipment, email and information systems available within school.
- All pupils in KS1 and above have a unique, individually named user account and password for access to IT equipment and information systems available within school. Reception class access the school systems via a shared password.
- All staff and pupils have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- We maintain a log of all accesses by users and of their activities while using the system in order to track any online safety incidents. Class teachers closely monitor the use of the internet by pupils in school.
- Passwords must be difficult to guess and should be a mixture of upper case and lowercase, numbers and symbols.

AWAITING APPROVAL 25/10/26 LGB MEETING

15. Filtering and Monitoring

15.1 Filtering

In order to ensure that appropriate online filtering is in place across our network, Clayton St John use Smoothwall Filter, a cloud-based web filter which is designed specifically for schools. The Smoothwall Filter system filters all internet feeds, across all devices and operating systems.

Smoothwall Filter blocks internet access to harmful sites and inappropriate content, meeting all of the technical requirements set out by the Department for Education and specifically blocking access to illegal content including child sexual abuse material.

Smoothwall Filter identifies the device/IP address (and where possible the individual), time and date of attempted access and the search term or content being blocked. It is customisable to ensure the provision meets the ongoing needs of our pupils and our staff.

We have support via a managed IT service desk whose staff are trained on the Smoothwall Filter system and can make real-time changes should a site need to be blocked/un-blocked urgently.

As an additional check, the DSL checks that our internet filtering is effective in blocking certain harmful material by using http://testfiltering.com/.

Smoothwall have been members of the Internet Watch Foundation since 1st June 2007.

15.2 Monitoring

As an additional safeguard we have keystroke monitoring in place through Smoothwall Monitor, who have been a member of the Internet Watch Foundation since 1st June 2007.

Smoothwall Monitor is a real-time, digital monitoring solution that flags safeguarding incidents as they happen when users view or type harmful content. This can capture activity that may indicate a risk, even outside of the regular web browser – such as in a Microsoft Word document etc. Smoothwall Monitor uses a combination of artificial intelligence and human moderation to determine the level of safeguarding risk.

Smoothwall Monitor alerts are accessible through a dashboard with higher level risks also reported to the DSL via an email alert so that a safeguarding response can be implemented. Where there is an immediate risk of harm, Smoothwall Monitor will phone the school to ensure prompt action. It is customisable to ensure the provision meets the ongoing needs of our pupils and our staff.

In line with the expectations set out within KCSIE, we will conduct an annual review of our filtering and monitoring arrangements which includes both technical and safeguarding expertise. This will be formally document and presented to the Local Governing Body.

AWAITING APPROVAL 10/10/26 LGB MEETING

16. Using the Internet and Email

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance Clayton St John's management information, safeguarding and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Communication by email between staff and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained.

All email activity is recorded in line with data protection laws. The school can view these records in situations where this is called upon.

As part of the curriculum, pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

Clayton St John will set clear guidelines about when pupil-staff communication via email is acceptable and staff will set clear boundaries for pupils. Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email address.

Please see the BDAT Acceptable Use of ICT Policy for further information.

AWAITING APPROVAL T3/10/26 LGB MEETING

17. Use of Generative Artificial Intelligence

At Clayton St John, we acknowledge that generative AI platforms are becoming commonly used by both children and adults. We are aware of and follow the DfE's guidance on this and we follow the subsequent principles:

- The use of any Gen AI in our setting (by staff or pupils) will be carefully managed by the school to ensure that users and their data are safe. This is governed by the BDAT Artificial Intelligence Policy.
- Staff are only permitted to use their school email account when using pre-approved Gen AI, and they must not enter data relating to children, staff or the school which is personal or sensitive.
- The school has a clear and well communicated approach to the use of any Gen AI (by staff or pupils), and this is aligned with the school's values and pedagogical approaches.
- To help users to safely use technology, we will talk about the use of these tools with pupils, staff and parents – their practical use as well as their safety and ethical pros and cons.
- We are aware that there will be use of these apps and exposure to Gen AI creations on devices at home for many pupils – these experiences may be both positive/creative and also negative (e.g. data breaches, misinformation, bullying, deepfakes, creation of deepfake intimate imagery and chatbots that encourage unhealthy and inappropriate relationships). Therefore, it is important as a school that we support pupils in developing digital literacy skills to help mitigate these risks.

18. Publishing Content Online

Clayton St John maintains editorial responsibility for any school-initiated website or publishing online to ensure that the content is accurate, and the quality of presentation is maintained. We maintain the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the website is the school address, e-mail and telephone number.

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring Clayton St John into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

We recognize that many aspects of the curriculum can be enhanced using multi-media and that there are now a wide and growing range of devices on which this can be accomplished.

Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Identities of pupils are always protected and, in line with GDPR regulations, parents have the option to opt out so that photographs of individual pupils are not published on the website without permission. Group photographs do not have a name list attached.

For their own protection, staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

We are happy for parents to take photographs at school events, except in specific circumstances where rights holders refuse permission, but will always make them aware that they are for personal use only and if they have taken photographs of children other than their own, they should not be uploaded to social media sites and can be only used for their personal use.

AWAITING APPROVAL 13/10/21 LGB MEETING

19. Training

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

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse other children online through:
    - Abusive, harassing, and discriminatory messages

  - Non-consensual sharing of nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

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

The DSL and safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

AWAITING APPROVAL 13/10/25 LGB MEETING

20. Policy Monitoring Arrangements

This policy will be reviewed every year by the Headteacher and ratified by the Local Governing Body. Given the ever-changing nature of technology, we will ensure that this review is supported by ongoing risk assessment which reflects current online safety issues that children face. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

We will monitor the impact of the policy using:

- Logs of reported incidents in the Online Safety and Filtering and Monitoring categories on CPOMS
- Internal monitoring data for network activity gathered through filtering and monitoring software
- Pupil, staff and parent voice

The policy will be published on the school website, shared with all staff and will be reflected in our IT Acceptable Use Policies for all stakeholders. We will provide a version in other languages if required.

21. Links to Other Guidance and Policies

This policy reflects existing legislation, including but not limited to The Malicious Communications Act 1988, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle

cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

It should also be read in conjunction with the following guidance and other BDAT/Academy specific policies:

- Keeping Children Safe in Education
- DFE Guidance on Relationships Education, Relationships and Sex Education and Health Education
- DFE Guidance on Teaching Online Safety in Schools
- DFE Guidance on Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- DFE Guidance on Searching, screening and confiscation
- DFE Guidance on Sharing Nudes and Semi-Nudes Advice for Education Settings
- Guidance for Safer Working Practice in Education Settings - February 2022
- DFE Digital and Technology Standards
- DFE Guidance on Mobile Phones in Schools
- NPCC Guidance for Schools on When to Call the Police

- BDAT Equality Statement and Objectives
- BDAT GDPR Policy
- BDAT Acceptable Use of IT Policy
- BDAT Social Media Policy
- BDAT Artificial Intelligence Policy

AWIATING APPROVAL 13/10/26 LOC MEETING

Appendix One: Summary of Policy Changes

The below table provides a summary of changes to this policy over time:

September 2024	
Page	**Summary of Change**

3	• Added in a greater range of examples of social media apps that are used by staff and pupils to more accurately reflect reality • Added in reference to Artificial Intelligence in recognition that there is a growing awareness and usage of this type of programme
4	Updated link to 2024 version of Ofcom report and the summary of its findings
5	• Updated statistics referenced to ensure they are accurate with the 2024 Ofcom report • Added in unpleasant behaviour/cyberbullying as one of the main issues schools are tackling on line to reflect current picture
9	Updated link to Safer Internet Video for Parents and Carers to the latest 2024 version
19	Updated all hyperlinks to the latest versions
September 2025	
Page	**Summary of Change**
2	Added reference to generative artificial intelligence into the summary of aims within the 'Trust Policy Statement' and the 'Introduction and Aims' section.
3	• Added in reference to DFE Guidance on Mobile Phones in schools and details of the approach taken in school to comply with this • Added in misinformation, disinformation (including fake news) and conspiracy theories into the 'Content' risks in line with the updated version of KCSIE.
4	Added in text from KCSIE that specifies the DSL as having overall lead responsibility for online safety including filtering and monitoring
4-5	Added in much greater detail about the safeguarding risks associated with generative AI
5-6	Changed the section about 'Ofcom's Children and parents media use and attitudes report' to reflect the 2025 findings rather than 2024. This includes updating the Primary only and Secondary only sections.
6	Added in Cybersecurity threats as a particular concern in education.
6-7	Added in link for governors to suggested questions around online safety
7	Added in that the Headteacher will have overall responsibility for the school's data management and information security
9-10	Added in section on the responsibilities of curriculum leaders (particularly in PSHE and Computing) in ensuring that proactive teaching of online safety underpins the whole-school approach
10	Moved signposting links for parents into the 'Raising Awareness with Parents About Online Safety' section.
11	Added more context as to the importance of the curriculum in educating pupils about online safety
12-13	Added in additional signposting links to reputable sources of supports for parents.
13-15	Inserted new section entitled 'Key Online Safety Issues' of which the existing cyberbullying section will now be a subsection. This will strengthen the policy as there are now further specific details about online sexual harassment, online extremism and social media incidents.
15-16	Made 'Searching and Screening' a standalone section to reflect that the procedures detailed may be applied in various situations, not just in cyberbullying cases where it was previously detailed.
16	Added in that pupils using school devices at home are still expected to follow the IT Acceptable Use Policy and that filtering and monitoring systems will still be in effect.

AWAITING APPROVAL 15/10/25 LGB MEETING

18	Updated the 'Filtering' section to reflect that it is now provided by Smoothwall Filter rather than Securly.
21-22	Added in information about where stakeholders can find this policy in the 'Policy Monitoring Arrangements' section and that a translated version can be made available if required.
22	Checked all hyperlinks and updated to the latest version of guidance where necessary

September 2026	
Page	**Summary of Change**
3	Updated the definitions of the four Cs of online safety to bring them into line with KCSIE 2026
4-6	Updated the information on online safety trends to reflect changes over the past year and new research by Ofcom and IWF.
11	Added in that staff will assess pupil progress in relation to online safety learning and provide additional support or intervention to those who may have gaps in knowledge. Added in reference to the DfE guidance on the use of screen time in the Early Years.
13	Strengthened section on adaptations for children with additional needs. Added in that safeguarding data and stakeholder feedback will be used to inform curriculum development.
14	Added in specific reference to generative AI being used to cyber-bully. Added in reference that advancing digital technology is also being used to facilitate sexual harassment in person (e.g. upskirting).
15	Added in additional section on nude and semi-nude images and how schools respond. This brings the Online Safety policy directly in line with the Safeguarding and Child Protection Policy.
16	Added in a reference to the forthcoming social media ban for under-16s. Added in that the Police may be called if an offence is committed when posting on social media.
18	Adapted section on mobile phones to reflect DfE Guidance on Mobile Phones in Schools. Added in that personal recording devices such as smart glasses are not permitted within school. Added in guidance around use of mobile devices on school trips.
20	Added in note to state that Smoothwall Monitor uses a combination of artificial intelligence and human moderation when assessing the level of risk
21	Added in a paragraph to reflect that school will complete an annual review of filtering and monitoring arrangements as required by KCSIE.
21-22	Added in new section on Use of Generative AI to ensure that the Online Safety Policy aligns with the BDAT AI Policy.
Throughout	Checked all hyperlinks and updated to newer versions of guidance where relevant

AWAITING APPROVAL 3/10/26 LGB MEETING