BENSHAM MANOR School

Online Safety Policy

Last reviewed: September 2026

Publication date: September 2026

Review date: July 2027

The latest version of this policy is available on the school website and upon request.

Governors have had oversight of this policy and review and approve it annually.

Contents

1. Introduction 3
2. Roles and responsibilities 3
3. Teaching online safety 5
4. Filtering and monitoring 6
5. Security 6
6. Educating parents and carers about online safety 7
7. Acceptable use agreement 7
8. Use of mobile and smart technology 7
9. Training and staff knowledge 8
10. Anti-Bullying and child-on-child abuse 9
11. Further information to support you 9

1. Introduction

Bensham Manor school is committed to a whole-school approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers, and governors. We use training, education, and effective procedures to educate, empower and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

In line with Keeping Children Safe in Education, we aim to address the following four areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, 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: Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying and
- commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The DSL takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. The DSL liaises with staff including the IT department, safeguarding team and outside agencies such as Entrust on matters of safety, safeguarding and welfare, including online and digital safety and when deciding upon a referral to relevant agencies.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of school life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

Our mechanisms to identify online safety concerns include our filtering and monitoring system, the direct work we conduct with pupils through our curriculum, the training we provide to staff, parents and carers.

Where online safety concerns arise we utilise our Safeguarding Policy, Acceptable Use Agreements and Behaviour Policy as necessary to ensure an appropriate response. This could include but is not limited to:

- intervention work with pupils on online safety,
- adjustments to the curriculum to teach key ideas or strategies for staying safe online,
- the use of the Behaviour Policy,

Where necessary, we may need to escalate concerns around online safety. The Designated Safeguarding Lead would take a part in this decision-making process and where necessary external agencies would be involved.

2. Roles and responsibilities

2.1 The governing body

- Take overall responsibility for this policy and its implementation
- Read, and understand this policy
- Understand the role of the Designated Safeguarding Lead and their deputies in online safety processes, and filtering and monitoring systems
- Ensure the policy is reviewed and updated annually
- Ensure students are taught about online safety
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated
- Ensure online safety is a running and interrelated theme whilst devising and implementing the whole

school approach to safeguarding and related policies and procedures

- Ensure appropriate filtering and monitoring systems are in place and ensure a documented review of their effectiveness is undertaken at least annually.
- Understand how parents have been engaged in the process of creating/updating this policy.
- Ensure the school has appropriate cyber security systems in place.

2.2 Headteacher

- Ensure staff understand this policy
- Ensure the policy is reviewed and updated annually
- Ensure the implementation of this policy is consistent across the school
- Ensure any new members of staff learn about our approach to online safety at induction and regularly thereafter
- Ensure students are taught about online safety
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns
- Ensure reviews are carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support at least once per academic year.
- Ensure the school has appropriate cyber security systems in place.

2.3 Designated Safeguarding Lead

- Support the headteacher in implementing this policy
- Oversee the annual review of the school's approach to online safety, supported by the setting's Prevent risk assessment and annual risk assessment that considers and reflects the risks that children face online.
- Take the lead responsibility for online safety as part of their duties as safeguarding lead
- Work with the headteacher, IT department, DDSLs, LGfL and Entrust to address any online safety concerns or incidents, in line with our child protection and safeguarding policy
- Liaise with external safeguarding partners as necessary, including children's social care and the police and make referrals with the support of relevant colleagues and their expertise
- Ensure any online safety incidents are recorded appropriately and that staff are aware of how to record online incidents
- Deliver staff training on online safety
- Provide regular updates regarding online safety incidents to the headteacher
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received
- Provide information for parents about the filtering and monitoring systems used by the school on all devices and networks

2.4 Network/ICT Manager

- Ensure appropriate filtering and monitoring systems are put in place
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online
- Ensure that the school's ICT systems are secure and protected against viruses and malware
- Ensure that the school has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

- Ensure filtering and monitoring systems block harmful and inappropriate content without unreasonably impacting teaching and learning

2.5 All staff and volunteers

- Read and understand this policy
- Assist with the consistent implementation of this policy
- Agree with and follow our acceptable use of IT agreement
- Agree with and follow the Staff Code of Conduct which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Understand the expectations, applicable roles and responsibilities of members of staff in relation to filtering and monitoring, be aware of indicators of possible abuse, neglect, exploitation or harm identified through technology use, and know how to report concerns in line with school safeguarding procedures
- Refer any online safety safeguarding concerns to the DSL or a Deputy DSL by using My Concern
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here' and not dismissing any reports.
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.

2.6 Parents and Carers

- Understand the importance of children being safe online
- Read, understand and comply with this policy
- Read the information shared with parents regarding acceptable use, what the school asks the child to be doing online, including the sites they will be asked to access and who from the school (if anyone) will be interacting with their child
- Read the information shared with parents regarding the school's filtering and monitoring systems
- Notify a member of staff regarding any questions regarding this policy and its implementation
- Ensure their child has read, understood and agreed to the acceptable use of IT agreement
- Support their child to behave safely and appropriately online

3. Teaching online safety

In line with 'Teaching online safety in school', published by the Department for Education in January 2023, we teach pupils about online safety and harms. Our teaching covers the underpinning of knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app they are using. We recognise the rapidly evolving nature of the online environment. Pupils will be supported to develop critical thinking skills and understand how misinformation, disinformation, conspiracy theories, algorithmic influence, persuasive design and emerging technologies, including artificial intelligence, can affect their decisions, wellbeing and safety online.. These skills are covered in CDM (Computer Digital Media lessons) , Extended Online Safety Tutor times, PSHCE and, as required, online safety 1:1 sessions with the Head of IT.

Throughout this, teachers and TAs will address online safety and appropriate behaviour in an age and developmentally appropriate way that is relevant to their pupils' lives, including:

- how to evaluate what they see online
- the risks posed by social media platforms
- how to recognise techniques used for persuasion
- online behaviour
- how to identify online risks
- how and when to seek support
- how elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online

● how elements of online activity can adversely affect a pupil's wellbeing

3.1 Pupils with additional vulnerabilities

We recognise that there are some pupils, for example those with special educational needs, children in care, previously looked-after children, children experiencing mental health difficulties, and children who have experienced abuse, neglect or exploitation who may be more susceptible to online harm.

Such groups may also face additional risks, for example from bullying, grooming and radicalisation. We tailor our curriculum to meet the needs of these pupils by having a clear and concise message when learning about online safety, ensuring understanding and that the material is pitched at a suitable level due to the students development. We will ensure these pupils receive the information and support they need through Online Safety Extended Tutor Times, discussions and CDM lessons.

In addition, our school completes an annual risk assessment for online safety. We consider the updated non-statutory guidance (January 2023) from the DfE on teaching online safety and how we teach these elements.

4. Filtering and monitoring

Bensham Manor School uses LGfL and Entrust as a filtering and monitoring system. This filters and monitors for any unsuitable or unwanted content. This covers our school network and the following devices: Desktops, Laptops, Chromebooks and iPads.

The DSL has lead responsibility for understanding the filtering and monitoring systems and processes in place. The DSL and deputies monitor the effectiveness of this system through the use of testfiltering.com. The DSL is supported by a governor in executing this duty. The governor is Stella Bryan.

The school takes care not to 'over-block' content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment and as required by the Prevent Duty.

The DfE has published filtering and monitoring standards (September 2026) which set out that schools should:

● Identify and assign roles and responsibilities to manage filtering and monitoring systems

● Review filtering and monitoring provision at least annually

● Block harmful and inappropriate content without reasonably impacting teaching and learning

● Have effective monitoring strategies in place that meet their safeguarding needs

We at Bensham Manor School have done the following in relation to this:

● Have clear roles and responsibilities in regard to Filtering and Monitoring in the school staff

● Audit completed annually, termly meetings held between the DSL and the IT manager

● Consider blocking in the termly meetings and when required to ensure that teaching and learning is not impacted

● Entrust is a highly effective system and their termly reports are shared with the IT manager, the safeguarding team and the safeguarding governor.

When the filtering and monitoring system detects usage that is concerning, we will record this in My Concern and take appropriate action, contacting parents and carers and also including a referral to children's social care when necessary.

For more information on filtering and monitoring, parents and carers can contact the DSL - Kirstie Byrne - kirstiebyrne@benshammanor.com

5. Security

Bensham Manor School has appropriate levels of security protection, and this is reviewed periodically to keep up with evolving cyber-crime technologies. This includes Police CyberAlarm.

6. Educating parents and carers about online safety

We recognise that parents can play a significant role in keeping their children safe online. To raise parents' awareness of online safety, we raise parents' awareness of internet safety in the parent and carer communication update, letters or other communications home, and in information via our website.

Online safety will also be covered during other parents' and carers events.

7. Acceptable use agreement

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet and use of mobile and smart devices. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. For further information on acceptable use, please refer to the separate agreements which detail our policy on personally owned devices, their use on premises and what is acceptable. In line with KCSIE paragraph 170 All schools should be mobile free environments by default.

8. Use of mobile and smart technology

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school, can sexually harass, abuse, bully or control their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. To manage this and reduce risk, pupils may bring mobile devices into school, but must keep them in their bag powered off during the school day, which includes after school clubs / trips and sports. Pupils must not turn the phones on under any circumstances. Should they need to make contact with home they must ask a staff member to do this for them. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action, which will result in the confiscation of their device. Students are not to access any social media platforms on a device within the school grounds, if doing so, the student is at risk of their device being removed for a period of 7 days.

Our Staff Code of Conduct outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.

In summary in relation to tablets, game, consoles, mobile phones and wearable technology we outline the following for each group:

Staff

- Mobile phones must be kept locked away or in bags during lessons. They can be used at break and lunch time in the staff room/class room. They must not be used in the toilet.
- If you are awaiting an urgent call/appointment, please let the Headteacher know and ensure your phone is on vibrate.
- Smart watches must not be accessed (other than for telling the time) when with pupils.

Pupils

- All devices are turned off and are kept within the students' bag
- The device can only be turned on once the student has left the school property, this includes when sitting on school transport waiting to leave the school site.
- If a student needs to contact a parent or carer, a member of staff will help them to do this.
- These rules apply to phones, tablets, game consoles and wearable technology and would also apply to any new technology which allows students to access the internet whilst in the school grounds
- If the students are on a school trip - this would also count as being in the school grounds and the same rules would apply.

Parents and Carers

- To take an active interest in the online life of their child, discussing who they are spending time with online and what platforms they are using.

- Share any concerns with school staff about inappropriate behaviour online.
- Work with school to support the young people to develop appropriate behaviour regarding to online activities.

To safeguard pupils and staff whilst also maintaining privacy, wearable technology of any kind—including smart glasses and other web-enabled or image-capturing devices—must not be brought onto or used on the school site; this applies to the whole school community - parents, carers, students and visiting professionals.

In terms of the appropriate use of social media, we outlined the following for each group:

Staff

Staff should avoid mention of the school, pupils and colleagues on their personal profiles on these sites. Any mention of the school, pupils, parents or colleagues deemed to be negative, critical or derogatory will be regarded as gross misconduct and the Governors will take disciplinary action. Please see the schools Social Media Policy for more information.

Pupils

To follow the school rules of SAFE / READY / KIND when being online.

To not engage with any online activities with people that they do not know.

To not give any personal information to others, or give away the personal information of peers or staff members.

Parents and Carers

To support their children to use social media appropriately and for positive use. To take an active interest in their child's online life and to regularly monitor the use of social media on their child's devices.

9. Training and staff knowledge

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. This will also include training on the filtering and monitoring system used by the school and an understanding of expectations, applicable roles and responsibilities in relation to this.

All staff members will receive refresher training at least annually as part of our safeguarding training programme, as well as regular updates where relevant (through training, safeguarding briefings and staff communication update).

The DSL and Deputy DSLs 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. This will equip staff with the relevant knowledge and skills to safeguard children effectively, including online.

All staff should be aware and know:

- The indicators of abuse, neglect and exploitation, understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the school procedures.
- That technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline.
- That children can abuse other children online, this can take the form of:
    - Online abuse, including sexual
    - Online harassment, including sexual
    - Cyberbullying
    - Misogynistic/ misandrist messages,
    - the non-consensual sharing of nudes and semi-nudes, including those generated by AI images.

- the sharing of abusive images and pornography with those who do not want to receive such content.

- That child-on-child abuse could be happening in the school setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

10. Anti-Bullying and child-on-child abuse

We recognise that our approach to online safety should strengthen the work we do around anti-bullying. The anti-bullying approach of the school is to 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.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying. This includes personal, social, health and economic (PSHCE) education, and other subjects where appropriate.

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

The school also publishes information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. The School also offers access to an online resource containing tips and information about Online Safety and how to spot signs of bullying or other inappropriate forms of communication. The school supports parents and carers with information and guidance about the use of social media and when specific alerts are sent out, these are shared within the wider school community.

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

We recognise that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children would have the capacity to

- Sexually Harass
- Abuse
- Bully
- Control others via the media and smart technology
- Share indecent images consensually and non-consensually (often via large chat groups)
- View and share pornography and harmful content

To manage this and reduce risk, pupils may bring mobile devices into school, but must keep them in their bag powered off during the school day, which includes after school clubs / trips and sports. Pupils must not turn the phones on under any circumstances. Should they need to make contact with home they must ask a staff member to do this for them. Any breach of the acceptable use agreement by a pupil may trigger disciplinary action, which will result in the confiscation of their device. Students are not to access any social media platforms on a device within the school grounds, if doing so, the student is at risk of their device being removed for a period of 7 days.

In addition, we understand that online behaviour can also constitute child-on-child abuse. We respond to incidents of child-on-child abuse in line with our Safeguarding Policy and Behaviour Policy, this includes the possible confiscation of devices while concerns are being addressed, discussions with students, parents and carers, the involvement of external agencies as and when required.

11. Further information to support you

We work with our local safeguarding partners to ensure our students are safeguarded. We will liaise with

these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

For parents the following websites could be of use

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- CEOP - how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed here

For students the following websites could be of use

- Mind- mental health support
- Togetherall- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app
- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For all staff and volunteers it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use

- UK Safer Internet Centre- practical resources, advice, and training to support safe and responsible internet use.
- internetmatters.org – research, free lesson plans, and resources to support the teaching of online safety and digital literacy across subject areas.
- DfE guidance Teaching online safety in schools - non-statutory guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Policies/ guidance to be read and understood alongside our online safety policy:

- Safeguarding/ Child Protection policy
- Behaviour policy
- Staff Code of Conduct including the acceptable use of technology
- Use of Artificial Intelligence - Bensham Manor policy
- Staff disciplinary procedures
- Anti-bullying procedures including cyberbullying
- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology in schools and colleges (DfE)
- Complaints procedure