



BENSHAM MANOR *School*

Online Safety Policy

Last reviewed: July 2025



AIMS

Our school aims to:

- 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [Filtering and Monitoring](#), [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's guidance on [protecting children from radicalisation](#). It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), [the Online Safety Act 2023](#) 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.

ROLES AND RESPONSIBILITIES

THE GOVERNING BOARD

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). The designated governor for online safety is [Stella Bryan](#).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

THE HEADTEACHER

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

THE DESIGNATED SAFEGUARDING LEAD

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, IT Network Coordinator, teachers, TAs and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the

school behaviour policy

- Updating and delivering staff training on online safety, Liaising with other agencies and/or external services if necessary
- Embedding the key principles outlined in Filtering and Monitoring (KCSIE 2023)
- Embedding the principles of the Sharing nudes and semi-nudes: advice for education setting - March 2024
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Liaise with local safeguarding partners and follow their policies and procedures where concerns are identified, including making referrals in line with the Safeguarding Policy where necessary.

This list is not intended to be exhaustive.

THE IT NETWORK COORDINATOR

The IT Network Coordinator is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a continuous basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensuring that the Schools Technician is aware of and complies with the relevant guidelines.

This list is not intended to be exhaustive.

ALL STAFF AND VOLUNTEERS

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's 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 and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Understanding that children with SEND face additional risks, for example, from bullying, grooming and radicalisation and that they will be supported to stay safe online.

This list is not intended to be exhaustive.

PARENTS / CARERS

Parents / carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy and liaise with the school around any suggestions for development
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents and carers can seek further guidance on keeping children safe online from the following

organisations and websites:

- What are the issues?, UK Safer Internet Centre
<https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2024/parents-and-carers/finding-out-more-about-specific-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>

VISITORS AND MEMBERS OF THE COMMUNITY

Visitors and members of the community who use the school'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.

EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum.

Pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Keep themselves safe online and that this is tailored to the needs of SEND students and those who have been victims to abuse.

Our approach to online safety is framed by four main areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as

The safe use of social media and the internet will also be covered in other subjects where relevant.

- 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 (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying)
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Bensham Manor follows the Government guidance to implement Online Safety in our school:

<https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools>

Our Safeguarding Curriculum Map is available in the Safeguarding section of our website:

<https://www.benshammanor.co.uk/wp-content/uploads/2022/10/Safeguarding->

Lessons are adapted and tailored to meet the needs of the students in the school, taking into account their special educational needs and EHCPs. We recognise that children with SEND face additional risks, for example, from bullying, grooming and radicalization and our curriculum is designed to support our pupils.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

The students have regular Extended Tutor Times when various aspects of Online Safety are discussed in addition to the lessons in CDM - Computer Digital Media. External agencies work alongside staff to promote awareness of how to keep safe online.

EDUCATING PARENTS / CARERS ABOUT ONLINE SAFETY

The school will 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 parents' evenings.

If parents or carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Designated Safeguarding Lead

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, where the relationship involves an imbalance of power.

PREVENTING AND ADDRESSING CYBER-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.

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
- 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

CAMERA / IMAGE USE

Students are not allowed to access their mobile devices to take any photos or videos of other students when on school grounds. Students are not allowed to access any social media apps and platforms either on their own devices or using school devices or computers.

Students using their phones or mobile devices to take photos or video of other students will have their devices confiscated for 7 days.

EXAMINING ELECTRONIC DEVICES

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, 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 DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or • Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

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

In line with the Safeguarding policy, no member of staff will view a child's device if there is thought to be an inappropriate image (such as a nude, or 'pic') on the device. Staff will follow the procedures set out in the Safeguarding policy.

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. This would also include the use of the school

internet system when accessing remote education. Visitors will be expected to read and agree to the school's terms on acceptable use where relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We actively monitor the websites visited by pupils, staff, volunteers, governors and visitors to ensure they comply with the agreements. Sanctions can be placed on any member of the Bensham community should they be found to be accessing inappropriate content, depending on the status of the community member.

PUPILS USING MOBILE DEVICES IN SCHOOL

Bensham Manor School recognises the requirements of parents / carers wishing their child to carry a mobile device in case of emergency. 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 / 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 may 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.

Rules for use of Mobile Devices in school:

- 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.

FILTERING AND MONITORING

Bensham Manor School uses LGfL as a filtering and monitoring system. This filters and monitors for any unsuitable or unwanted content. Bensham Manor also uses SupportNet DNA to further filter and alert the Safeguarding team of any inappropriate use of the school internet system. This covers our Bensham Manor School network and the following devices: 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 termly meetings with Stuart Woolley - Head of IT to discuss generated reports on filtering.

Bensham Manor School takes care to not '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 as required by the Prevent Duty.

The DfE has published [filtering and monitoring standards](#) 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 reasonable impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

At Bensham Manor School have done the following in relation to this: Staff have attended training with LGfL, DSL and Head of IT hold regular meetings.

When the filtering and monitoring system detects concerning usage, the DSL, Kirstie Byrne will record this and take appropriate action, including a referral to children's social care when necessary.

For more information on filtering and monitoring, parents and carers can contact Stuart Woolley or Sean Fitzgerald - ITservices@benshammanor.com

Bensham Manor School has also provided links to Schoolsmobile.com which can block unwanted content from students' devices. Online meetings and drop in clinics are continuing to be held for parents and carers.

STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff Members have been issued with digital devices and may take them home. Agreements have been signed to cover this. Tablets, Laptops and Mobile phones should be password protected and should not be shared by members of family due to potential data breaches. The school recommends best practice anti-virus and malware protection software and offers advice on maintaining the device where appropriate. The use of USB devices to transfer data between home and work is now forbidden and all data sharing should be done via the schools Google Suite Accounts. If staff have any concerns over the security of their device, they must seek advice from the IT Network Coordinator.

Irrespective of what device the staff member is using, Bensham Manor expects all staff to use social media responsibly and not use social media to bring the school into disrepute. All staff are expected to follow the Bensham Manor staff code of conduct at all times and failure to do so could lead to disciplinary action.

Work devices must be used solely for work activities.

SHARING NUDES AND SEMI-NUDES

What do we mean by sharing nudes and semi-nudes?

In the latest advice for education settings (UKCIS, 2024), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18.

Nudes and semi-nudes can be shared online via social media, gaming platforms, chat apps, forums, or involve sharing between devices using offline services. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nudes are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to the attention of a member of staff:

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately.

Follow the Bensham Manor Child Protection and Safeguarding Policy.

- Never view, copy, print, share, store or save the imagery, or ask a child to share or download – this is illegal.
- If a staff member has already viewed the imagery by accident (e.g. if someone has shown it to them before you could stop them), report this to the DSL (or equivalent) and seek support.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).

- Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the Behaviour Policy. 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 school's ICT system 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. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

TRAINING

All staff should be aware of indicators of abuse and neglect and understand that children can be at risk of harm inside and outside of the school and inside and outside of the home and online.

We train all staff to understand this and to be aware 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.
- 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 incident images, especially around chat groups,
 - and the sharing of abusive images and pornography to those who do not want to receive such content.

All staff should know that child-on-child abuse could be happening in the school setting and that this could be taking place online. Staff must report any cases of child-on-child abuse in line with our safeguarding procedures.

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

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).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years as a minimum but the safeguarding team at Bensham Manor update their training every year. They will also update their knowledge and skills on the subject of 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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

LINKS WITH OTHER POLICIES / DOCUMENTS

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- IT Equipment Signing Out Form
- The Prevent Duty

This policy will be reviewed regularly, and at least annually, to ensure it remains relevant in the advent of new technologies.

This policy is available on the school website and access for staff is in the Policy library and within the Safeguarding Folder on Google Drive.