



Online Safety Policy

September 2026

1. Aims

Birtley House School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers
- 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 and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Birtley House believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Birtley House identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content-** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact-** being subjected to harmful online interaction with other users, such as 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, such as 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; and
- **Commerce-** risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

[Teaching online safety in schools](#)

[Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)

[Relationships and sex education](#)

[Searching, screening and confiscation](#)

It also refers to the DfE'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](#) 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.

This policy also takes into account the National Curriculum computing programmes of study.

This policy must be read in conjunction with other relevant school policies including (but not limited to) child protection, anti-bullying, behaviour, social media, acceptable use and confidentiality.

See Appendix 6 for information on Birtley House School's Filtering and Monitoring process.

Online Safety Policy – September 2026

TO BE REVIEWED: September 2027 or as needed

3. Roles and Responsibilities

3.1 Directors

The Directors have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Directors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Ensure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness (Appendix 6)

The Director will review DfE filtering and monitoring standards, and discuss the IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities.

3.2 The Headteacher and Senior Leadership Team

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

The Senior Leadership Team are responsible for:

- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology
- Ensuring that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- Working with and supporting technical staff (John Turnbull) or KCC internet Service in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored
- Being aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice
- Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices

3.3 The Designated Safeguarding Lead (and Deputies)

- Designated Safeguarding Lead: Ms P Rahman
- Deputy Safeguarding Leads: Mrs Ellie Austin, Mrs Sarah Whelan

The DSL and Deputies take lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the SLT to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Working with staff to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Ensuring that any online safety incidents are logged on the CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the school behaviour policy and anti-bullying policy
- Updating and arranging the delivery of staff training on online safety (appendix 4 – self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services including the local authority and other local and national bodies, as appropriate
- Keeping up-to-date with current research, legislation and trends regarding online safety
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches
- Providing regular reports on online safety in school to the Governing Board.

3.4 Technical Support Staff

- 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 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

3.5 All staff and volunteers

All staff, including contractors 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

Online Safety Policy – September 2026

TO BE REVIEWED: September 2027 or as needed

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting it to the DSL
- Reporting any suspected breaches to a DSL if they need to bypass the filtering and monitoring systems for educational purposes
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school anti-bullying policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Their own professional development in this area
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery where possible
- Maintaining a professional level of conduct in their personal use of technology, both on and off site

3.6 The children

All children, at a level that is appropriate to their individual age, ability and vulnerabilities, are responsible for:

- Respecting the feelings and rights of others both on and offline
- Seeking help from a trusted adult if things go wrong
- Keeping themselves and others safe online
- Their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks

3.7 Parents and/or carers

Parents and/or carers are expected to:

- Notify a member of staff of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- Role model safe and appropriate uses of technology and social media

Parents and/or carers are expected to:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet - [Childnet International](#)

3.8 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 are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3)

4. Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- 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

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents and/or carers about online safety

Birtley House School will raise parents' and/or carers awareness of internet safety in letters and other communications home, and in information via our website. This policy will also be shared with parents.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- 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 and/or carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff.

6. Cyber-bullying

6.1 Definition

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. (See also the school behaviour policy and anti-bullying policy.)

6.2 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 a victim.

Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy and behaviour 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.

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

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search 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 an 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:

- Make an assessment of 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
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions
- Seek the pupil's co-operation

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
- Commit an offence

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*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- 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.

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

- **NOT** view the image
- Confiscate the device and report the incident to the DSL 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](#)

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Birtley House School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Birtley House School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and if any AI tools were used by school a risk assessment would be required.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and members of the Governing Board are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2 as well as the Staff Acceptable Use Policy). Visitors will be expected to read and agree to the school's terms on acceptable use if 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.

Online Safety Policy – September 2026

TO BE REVIEWED: September 2027 or as needed

We will monitor the websites visited by pupils, staff, volunteers, Directors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Online Communication and Safer Use of Technology

8.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE)
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published
- The school will post information about safeguarding, including online safety, on the school website for members of the community

8.2 Managing emails

- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider. Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding records
- Any electronic communication which contains any content which could be subject to data protection legislation will only be sent using secure and encrypted email
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored
- Emails sent to external organisations should be written carefully and authorised before sending
- School email addresses and other official contact details will not be used for setting up personal social media accounts

9. Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational.

9.1 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items
- The sending of abusive or inappropriate messages or content is forbidden by any member of the community and any breaches will be dealt with as part of the behaviour policy
- Everyone will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's policies

9.2 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children and their families within or outside of the school in a professional capacity
- Staff will not use personal devices to take photos or videos of children and will only use work-provided equipment for this purpose
- Staff personal mobile phones and devices will be switched to 'silent' mode during lesson times
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances

- If a member of staff breaches the school policy, then disciplinary action will be taken
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, then the police will be contacted

9.3 Staff using work devices outside of school

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
- 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

9.4 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors

9.5 Children's use of personal devices and mobile phones

- Children are not permitted to bring personal devices or mobile phones to school or to use them on the school premises, except under a pre-organised arrangement with the Headteacher. Cases will be looked at on an individual basis
- If an arrangement has been made for a child to bring a personal device or mobile phone to school, it will remain switched off and handed to a teacher

10. Digital Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals.

When using digital images:

- Staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes

11. 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 our behaviour policy, acceptable use policy, and anti-bullying 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 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/staff code of conduct. 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.

12. 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 online safety refresher training at least once each academic year 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 their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent 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 deputies 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 on the subject of online safety at regular intervals, and at least annually.

Directors 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.

Birtley House School
Acceptable use of the school's ICT systems and internet: Pupils

All pupils use online facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.

Pupils have access to online resources using computers, tablets and other computing resources.

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for education purposes only
- Always ask permission from an adult before using the internet
- Only use websites and search engines that my teacher has chosen
- Use school computers for school work, unless I have permission otherwise
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I am finished working on it
- Only send messages which are polite and friendly
- Only talk with and open messages from people I know and I only click on links if I know they are safe

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is offensive, obscene or inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	Date:
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	Date:

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: Name of child:
I, with my child, have read and discussed Birtley House School Pupil Acceptable Use Policy. I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the school’s systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation. I, with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community. I understand that the school will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed through the internet. I understand that my child’s activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child’s safety. I will inform the school or other relevant organisations if I have concerns over my child’s or other members of the school communities’ safety online. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school. I will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • be respectful towards members of staff, and the school, at all times • be respectful of other parents/carers and children • direct any complaints or concerns through the school’s official channels, so they can be dealt with in line with the school’s complaints procedure I will not: • use private groups or personal social media to complain about or criticise members of staff. This is not constructive and the school can’t improve or address issues if they aren’t raised in an appropriate way • use private groups or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I’m aware of a specific behaviour issue or incident • upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children’s parents/carers

Signed (parent/carer):	Date:
-------------------------------	--------------

Appendix 3

Acceptable use agreement (Staff, Directors, volunteers and visitors)

As a professional organisation with responsibility for children’s safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

Name:

When using the school’s ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school’s reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network
- Share my password with others or log in to the school’s network using someone else’s details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I’m not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school’s ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/Director/volunteer/visitor):

Date:

Appendix 4

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Online Safety Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Kent Police:

www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kent e-Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/online-safety

Parent Port: www.parentport.org.uk

Online Safety Policy – September 2026

TO BE REVIEWED: September 2027 or as needed

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: <http://www.mariecollinsfoundation.org.uk/>

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: <https://360safe.org.uk/>

Online Compass (Self review tool for other settings): <http://www.onlinecompass.org.uk/>

Filtering and Monitoring Processes

Filtering

Birtley House School employs Medway Grid for Learning who provide the following:

- Layer 7 Firewalling and zero day threat protection with Palo Alto Firewalls
- High speed Internet connectivity with Cisco switches and routers
- Internet content filtering with Smoothwall Web Filter
- Cisco Email SPAM filtering
- Remote Access into the school LAN with Junos Pulse VPN

(see Appendix A for more detail)

The Firewalls have additional features that block attacks.

The Spyware prevents PCs from transmitting data or ransomware encrypting files.

URL filtering adds additional protection for threats not blocked by Smoothwall.

The specific decisions about the filtering systems used were taken by Medway Grid for Learning who provide these services to hundreds of schools across Kent and other Boroughs.

PCs / laptops are accessed via individual pupil or and teacher login so that when any filtering concerns are reported via the smoothwall system the specific pupil / staff member is identifiable.

The ipad filtering is managed by the URL, dynamic content analysis and additional monitoring.

All our pupils have SEND therefore they are particularly vulnerable. Staff carefully monitor all access to PCs, Chromebooks, laptops and ipads in high staff:pupil ratio settings of no less than 6 pupils:1 staff. Pupils are never able to access equipment without direct supervision. Ipads and Chromebooks are locked away in a purpose designed security cabinet accessed via a key stored by a teacher.

We do not allow pupils to bring their own devices to school.

Monitoring

The DSLs are responsible for managing and escalating any safeguarding concerns. The DSLs work with the school IT technician, John Turnbull and Medway Grid for Learning, the school's Broadband provider and filtering provider to ensure that all pupils and stakeholders are kept safe using online resources and equipment in school.

Guidelines are also provided for online safety outside of school:

- Parents are encouraged to use child filtering controls on tvs / phones / /tablets / computers / laptops and other online devices
- Useful links are provided via the school website offering extensive information on parental controls, limitation of network filters, social media advice, guides to apps, privacy and identity theft and a wide variety of online issues

Smoothwall provides a daily monitoring report to the Headteacher (and DSL) and also instant reports of any attempted filtering breaches / concerns.

Once a term a filtering check is run using the site 'testfiltering.com' which monitors the content of the school online systems for – Child Sexual Abuse Content / Terrorism Content / Adult Content and Offensive Language Content. Copies of this are kept in the Child Protection and Safeguarding Folder.

To date (01/9/26), all potential sites of concern have been fully blocked.

Staff Meetings take place annually (or more frequently if required) to educate staff about the filtering and monitoring systems and so that staff know how to recognise and report a concern.