Aletheia Academies Trust

Online Safety Policy

September 2025

Company Number:	07801612
Approved By:	Board of Trustees
Policy Type:	Non-Statutory
Adopted On:	September 2025
Date of Next Review:	September 2026
Review Period:	One Year

Contents

1. Aims

Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- 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 (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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, antisemitism, 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 scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 Headteacher/Head of School 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 Online Safety Act 2023 and 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.

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

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1. The governing board

The local governing body has overall responsibility for monitoring this policy and holding the Headteacher/Head of School to account for its implementation.

The local governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The local governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The local governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The local governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The local governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with 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.

The Safeguarding Governor will oversee online safety as part of their role

All governors will:

- Ensure 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 (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college 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 (SEND). This is 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.

3.2. The Headteacher/Head of School

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

3.3. The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the Headteacher/Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher/Head of School and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks and routinely checking integrity/effectiveness.
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher/Head of School, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in school to the Headteacher/Head of School and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4. The ICT Support/Helpdesk

The ICT Support/Helpdesk is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 on a monthly 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 (see appendix 5) 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

This list is not intended to be exhaustive.

3.5. 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 this immediately to a DSL
- Following the correct procedures by contacting the IT Help Desk if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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
- 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'
- Engage with training and updates about new and evolving risks and threats to online safety. This includes, but is not limited to, understanding the Online Safety Act 2023 and its stronger protections for children online.

This list is not intended to be exhaustive.

3.6. Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher/Head of School 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 (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7. 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 (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

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

In **Key Stage 3**, 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, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the

way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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/Carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers.

Online safety may also be covered during parents' evenings.

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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/Head of School and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Head of School.

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour 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 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. Class teachers and form teachers will discuss cyber-bullying with their tutor groups.

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 (PSHE) 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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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 endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3. Examining electronic devices

The Headteacher/Head of School, and any member of staff authorised to do so by the Headteacher/Head of School (as set out in the School's behaviour policy, 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/Head of School or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school 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 / Headteacher / Head of School / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and

the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

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

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

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

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The behaviour policy

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

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.

The 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The School will treat any use of AI to bully pupils in line with our Anti-bullying/Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

6.5 New Offences set out in the Online Safety Act 2023

DSLs should help ensure these risks are understood by staff as safeguarding issues and addressed in training and policy.

The Act introduces new criminal offences.

- **Cyberflashing** - Illegal to send unsolicited sexual images intended to alarm or distress.
- **Epilepsy trolling** - Criminal to send flashing images aiming to trigger seizures or cause distress
- **Encouraging serious self-harm** - Offence to promote or encourage serious self-harm online, even if harm doesn't occur
- **Threatening communications** - Sending threats of serious harm, death or violence is a stand-alone offence.

- **Sharing intimate images (including deepfakes)** - Offence to share or threaten to share sexual images without consent, including AI-generated content.

These include cyberflashing, epilepsy trolling, and encouraging or assisting serious self-harm, which are now illegal even if done anonymously. It is also a crime to share deepfake pornography or send false information with intent to harm. Laws on non-consensual intimate images have been strengthened to cover threats to share, and images altered using AI.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them on the school premises during the school day as set out in the School's Behaviour Policy.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 3 and 4).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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

Work devices must be used solely for work activities.

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

10. 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 policies on Behaviour and ICT Acceptable Use Policies. 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

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

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

    (a) Abusive, harassing, and misogynistic messages

(b) Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

(c) 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 up the risks
- 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 their 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.

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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Trust Safeguarding Lead and ICT Manager and approved by the Board of Trustees. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1:

Facebook Cheat Sheet for Staff

Do not accept friend requests from pupils social media!!

10 Rules for Academy Staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, your colleagues, our academy or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at an academy event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.

10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils).

Check your Privacy Settings

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster.
- Google your name to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this
- Remember that some information is always public: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher/Head of School about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2:

Acceptable Use of the Internet: Agreement for Parents and Carers.

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: - Email/text groups for parents (for school announcements and information) - Our Website - Our official Facebook page Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
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, the school's Facebook page, 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 unless they are raised in an appropriate way.
- Use private groups, the school's Facebook page, 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 the other children's parents/carers.

Signed:	**Date:**

Appendix 3:

Acceptable Use Agreement for Older Pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers
Name of pupil:
When using the school's ICT facilities and accessing the internet in school, I will not: - Use them for a non-educational purpose - Use them without a teacher being present, or without a teacher's permission - Use them to break school rules - Access any inappropriate websites - Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) - Use chat rooms - 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 - Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video

- Share my password with others or log in to the school's network using someone else's details
- Bully other people

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

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

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 for using personal electronic devices in school, and will make sure my child understands these.

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

Appendix 4:

Acceptable Use Agreement for Younger Pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers
Name of pupil:
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: - Use them without asking a teacher first, or without a teacher in the room with me - Use them to break school rules - Go on any inappropriate websites - Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) - Use chat rooms - Open any attachments in emails, or click any links in emails, without checking with a teacher first - Use mean or rude language when talking to other people online or in emails - Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes - Share my password with others or log in using someone else's name or password - Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (Parent/Carer):	**Date:**

Appendix 5:

Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

Acceptable Use of the School's ICT Facilities and the Internet: Agreement for Staff, Governors, Volunteers and Visitors
Name of Staff Member/Governor/Volunteer/Visitor:

When using the school's ICT facilities 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
- 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 understand 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/Governor/Volunteer/Visitor):**	**Date:**

Appendix 6:

Glossary of Cyber Security Terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber Attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber Incident	Where the security of your system or service has been breached.

TERM	DEFINITION
Cyber Security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download Attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social Engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-Phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.

TERM	DEFINITION
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-Factor/Multi-Factor Authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 7:

Online Safety Training Needs – Self-Audit for Staff

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?	

Online Safety Training Needs Audit	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	

Appendix 8:

Online Safety Incident Report Log

Online Safety Incident Log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**