



Online Safety Policy

Our Vision

Achieving More Together

Our Mission

*Working together passionately to achieve the best outcomes
for children and young people in our specialist SEND & AP settings*

Reviewed by:	CEO & Director of Operations Reviewed on 31 st March 2026. It will be presented to the Education & Outreach Committee for ratification in April 2026.
Ratified by:	Education & Outreach Committee
Ratification Date:	30 th April 2026
Review Frequency: (Subject to Academy Trust or national policy change)	Annually
Review Date:	March 2027
Related Trust/School Policies:	- Internet Acceptable Use - Child Protection and Safeguarding Policy - Anti-Bullying Policy - Staff Code of Conduct - Positive Behaviour Policy - Data Protection Policy

Contents

1. Aims.....	3
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	4
4. Educating pupils about online safety.....	8
5. Educating parents/carers about online safety.....	10
6. Cyber-bullying	10
7. Acceptable use of the internet in school	12
8. Pupils/staff using personal mobile devices in school	13
9. Staff using work devices outside school	14
10. How the school will respond to issues of misuse	14
11. Training	15
12. Monitoring arrangements.....	16
Appendix 1: Acceptable use agreement for staff.....	15
Appendix 2: Acceptable use agreement for older pupils	18
Appendix 3: Acceptable use agreement for younger pupils (to be read with or differentiated for pupils where appropriate).....	19

Version control

No	Date	Changes
1	March 2025	Inroduction of trust-wide policy
2	March 2026	• Updated roles and responsibilities for clarity • Added references to misinformation / disinformation / conspiracy theories • Clearer reference to schools with stronger powers to search for and confiscate prohibited items • Updates on the use of personal devices in school • Wider reference to adults including staff, visitors and volunteers

1. Aims

All Enable Trust schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers
- 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
- Establish clear mechanisms to identify, intervene and provide support to ensure staff and pupils are following an acceptable use of technology

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, (misinformation / disinformation) conspiracy theories, 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, whilst recognizing that online abuse frequently co-exists with offline abuse, particularly in peer-on-peer contexts
- **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 2025, [Working Together to safeguard Children 2026](#), 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 provides schools with stronger powers to search for and confiscate prohibited items, including electronic devices, and 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 (see 6.3) and which is informed by current statutory safeguarding guidance including Keeping Children Safe in Education.

3. Roles and responsibilities

3.1 The Board of Trustees (the Board)

The Board is accountable for ensuring the safe and effective implementation of this policy and all associated procedures and holding the Headteacher to account for so doing.

All Trustees will complete online safety training to clarify their role and responsibilities and will comply with the Trust's IT acceptable use guidance.

The Board will ensure that all Trust schools have a registered IT provider who provides a secure school network and appropriate levels of filtering and monitoring across the network and on all school devices, in line with the DfE filtering and monitoring standards.

3.2 Trust Operations Team

Operational responsibility for the management of the IT contract rests with the Trust Operations team who will ensure that:

- Procurement processes for IT Support contracts include specifications requiring compliance with online safety and cyber security standards
- The IT Support contracts are managed appropriately to ensure compliance with online safety and cyber safety standards
- Filtering and monitoring provisions are in place and reviewed at least annually.
- Filtering and monitoring provisions block harmful and inappropriate content without unreasonably impacting teaching and learning.
- The Central Services Teams undertake online safety as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

3.3 Local Governing Body (LGB)

The LGB will appoint an Online Safety Governor who will provide regular scrutiny of the school's online safety procedures through reports from and meetings with school online safety leads and / or DSL. The LGB will feedback to the Board issues or challenges with effective implementation of this policy.

All Local Governors will complete online safety training to clarify their role and responsibilities and will comply with the Trust's IT acceptable use guidance.

3.4 The Headteacher

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

- 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.
- 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.
- Online safety logs are regularly monitored and actioned.
- Children are taught how to keep themselves and others safe, including keeping safe online.
- Online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- 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.
- School based staff are assigned to manage filtering and monitoring systems at a school level, including ensuring that all messages and alerts related to online filtering and monitoring are responded to and actioned.

3.5 The Designated Safeguarding Lead (DSL)

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 online safety lead in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the online safety lead and governing body 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
- Working with IT support to make sure the appropriate systems and processes are in place
- Working with the online safety lead, IT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing online safety issues alongside the online safety lead and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged using CPOMS, are dealt with appropriately, monitored to inform level of risk and to inform curriculum content.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately alongside the online safety lead and in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Undertaking annual audits that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to provide them with relevant skills and knowledge to safeguard effectively
- Reviewing effectiveness of filtering and monitoring annually with the IT support manager

3.6 The online safety lead

- Undertakes training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online
- Monitor their designated area on CPOMS and respond to incidents of online safety alongside the DSL
- Liaise with staff to support them in managing online safety concerns about their pupils
- Taking guidance from the DSL so that appropriate referrals are made to external agencies as required
- Keep up to date with current research, legislation and online trends
- Coordinate the school's participation in local and national online safety events e.g. Safer Internet Day
- Update and deliver staff training on online safety when necessary
- Provide regular online safety updates and resources to pupils, staff and parents throughout the school year
- Providing regular reports on online safety in school to the headteacher and/or governing body
- This list is not intended to be exhaustive
- Manage the 360 Safe audit

3.7 IT support

Enable Trust outsources IT Support to reputable external contractors. As part of the contract, the IT support team 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 IT 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 IT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Review filtering and monitoring systems and procedures annually with the DSL/online safety lead
- Ensuring that staff devices are 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates
- This list is not intended to be exhaustive.

3.8 All staff and volunteers

All staff including agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on the IT and Internet Acceptable Use policy (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:
 1. Closing (e.g. laptop) or removing a device if a breach has been identified
 2. Do not shut down, navigate away or investigate further
 3. Report directly to the DSL or online safety lead immediately
- Following the correct procedures by discussing with DSL/headteacher/ IT support manager if they need to bypass the filtering and monitoring systems for educational purposes

- Working with the DSL and/or online safety lead to ensure that any online safety incidents are logged on CPOMS 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'

This list is not intended to be exhaustive.

3.9 Parents/carers

Parents/carers are expected to:

- Read (with their child where appropriate), have understood and agreed to the terms of their child's acceptable use of the school's IT systems and internet by signing the acceptable use agreement. (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from:

- Online safety lead
- [UK Safer Internet Centre](#)
- [Childnet](#)
- [CEOP](#)
- [NSPCC](#)
- [Internet Matters](#)
- [Support and Advice for Parents and Carers on Synthetic Media & Deepfakes](#)

3.10 Visitors and members of the community

Visitors and members of the community who use the school's IT 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

Across the Trust pupils have differing levels of need. Each school within the Trust have their own learning pathways. Pupils will be taught about online safety as part of each school's curriculum in line with their level of need.

Further information can be obtained from individual schools.

All schools where appropriate to pupils SEND will teach pupils to:

- Use technology safely and respectfully, responsibly, 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
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact
- 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
- 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
- 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
- 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
- Keeping personal information safe
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That sexual material, naked images or computer-generated imagery should not be shared
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including police involvement and prison
- 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.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of online safety in letters or other communications home, and in information via our website or communication platforms. This policy will also be shared with parents/carers via the trust/school website.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with school staff, online safety lead and/or the DSL.

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.)

6.2 Preventing and addressing cyber-bullying

All pupils at Enable Trust have SEND and/or specific vulnerabilities and where able, to help prevent cyber-bullying, we will ensure that pupils can 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, where appropriate, cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Relationships, Sex and Health Education (RSHE) 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

Under the Education Act 2011, the headteacher/DSL, can search pupils and confiscate their mobile phones, computers or other devices if they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Contravenes the acceptable use policy and contains content that needs investigating/removing
- Is evidence in relation to an offence

Before a search, the DSL/DDSL should be 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.
- Explain to the pupil why their device is being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's consent (consideration to whether the pupil can give informed consent should be made)

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 DSL/DDSL 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, DSL/DDSL 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, DSL/DDSL 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 self-generated intimate images including AI deepfakes), 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](#)

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.

Enable Trust 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.

Enable Trust will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff and pupils should be aware of the risks of using AI tools whilst they are still being developed and should refer to the ICT and Internet Acceptable Use Policy for guidance.

See the Trust AI Policy and guidance for further information

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 IT systems and the internet (appendices 1 to 3) even if pupils do not have the cognitive ability to access the internet and social media independently. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. All parents/carers are expected to consent on Arbor after reading the online safety policy and acceptable use agreements (appendices 1 to 3).

Use of the school's internet must be for educational purposes only in directed time, 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. Staff and visitors need to be aware that if using the school guest Wi-Fi any existing tabs they have open from visiting websites may be subject to filtering and monitoring.

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

8. Pupils and adults (staff, visiting professionals and volunteers) using personal mobile devices in school

Pupils and adults may bring mobile phones, tablets, smart watches (without camera function) and other digital devices into school, **however;**

- **Pupils are not permitted to use personal devices during;**

- All lessons / unstructured time* (*see * below*)
- Clubs before or after school, or during any other activities organised by the school. e.g. school trips, including where they extend beyond the typical school day. *
- Home to school transport - The school discourages the use of personal devices during journeys to and from school where transport is arranged by the Local Authority. However, responsibility for pupils' use of devices outside school hours, including during travel, rests with parents/carers, unless otherwise supervised by school staff. For example, parents are expected to have guided access or other appropriate restrictions in place.

*Exceptions may be granted by the headteacher. For example;

- For individual pupils where there is a clear need, such as medical reasons.
- Where pupils require Augmentative and Alternative Communication (ACC) devices as part of their identified needs, these should be permitted as standard and recorded within the school's SEND or accessibility arrangements
- During school trips or visits, mobile device use may be permitted by exception, at the discretion of the trip leader or headteacher, where it supports safety, communication, or the educational purpose of the visit.

Each school will have their own local arrangements regarding such devices, such as collection, storage pouches etc. Any arrangements that work for the operational requirements of the school are acceptable, as long as the above protocols are followed.

- **Adults are not permitted to use personal devices during;**

- All lessons*
- Other directed time, such as staff meetings*
- Adults may use their devices during their breaks, but always away from pupils

*Exceptions may be granted by the headteacher. For example;

- Staff are permitted to log into CPOMS or other work-related applications, for example, if two factor authentication is required.

- Where adults do have permission to carry their mobile phone for a specific reason, they must remain out of sight and used only as agreed by SLT.

Where adults do have permission to use the school Internet using their own devices, they need to be aware that any open pages from previous and current internet browsing are subject to the schools filtering and monitoring.

Any use of mobile devices in school by pupils and adults must be in line with the IT and Internet acceptable use policy. Any breach of the acceptable use agreement by a pupil or staff member 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 are recommended (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the IT and Internet Acceptable Use Policy
- Work devices must be used solely for work activities
- If staff have any concerns over the security of their device, they must seek advice from their IT support team

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our behaviour policy and acceptable use agreement. 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 IT 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 and acceptable use agreement. 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 LADO or the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safety issues, including cyber-bullying, sexting, upskirting, sharing of indecent images including computer generated imagery, sharing personal information, social media, online hate, online abuse and exploitation including CSE, protecting privacy, cyber security, phishing and the risks of online radicalisation. This list is not exhaustive and will be updated as technology advances.

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:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of self-generated intimate images including AI deepfakes 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 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

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

12. Monitoring arrangements

School staff log behaviour and safeguarding issues related to online safety using CPOMS. This is monitored by the DSL/DDSL and online safety lead.

This policy will be reviewed every year by the designated DSL/online safety lead. At every review, the policy will be shared with the trust safeguarding team, governing body and trustees.

Each school will complete an online safety review – 360 Safe [here](#) and will be supported by an annual audit 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.

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carers:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school. Across the trust schools can use the following channels:

- School/Home communication platforms e.g. Seesaw
- Email/text groups for parents (for school announcements and information)
- Virtual learning platforms

Parents/carers may set up independent channels to help communication. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels such as school email addresses, 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 or any other Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues unless they are raised in an appropriate way
- Use private groups, the school or any other 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 2: Acceptable use agreement for older pupils

Acceptable use of the school's IT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's IT 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
- 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 self-generated intimate images including AI deepfakes, 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
- Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
 - During assessments, including internal and external assessments, and coursework
 - To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's IT 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 IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 3: Acceptable use agreement for younger pupils (to be read with or differentiated for pupils where appropriate)

Acceptable use of the school's IT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's IT systems (like computers or iPads) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: ○ I select a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school devices for school work only • Be kind to others and not upset or be rude to them • Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off when I have finished using it 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): (where applicable)	Date:
Parent/carer agreement: I agree that my child can use the school's IT 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 IT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	Date: