Online Safety Policy

(Incorporating Acceptable Use Appendices)

Date of issue:	September 2025
Responsible sub-committee:	Learner Experience Quality of Inclusion Finance & Resources
Linked policies:	Child Protection and Safeguarding policy School Behaviour and Search policies School Bullying Policies Disciplinary policy Data protection policy CCTV policy Complaints policy Code of Conduct Finance policy
Review Date:	September 2026 Annual review for any changes to KCSIE
Target audience:	All stakeholders (Staff, pupils, Trustees, governors, Members, parents/carers)
Dissemination via:	School websites / SharePoint

Version	Section	Amendments	Date	Author
1.0	Acceptable Use Social Networking Don'ts Title	Edit point 20 to include smart wear. Added point 21 Added point 10 Changed to Online Safety from E-safety	February 2020	L Askin
2.0	Acceptable Use	Added working from home	November 2020	L Askin
3.0	Teams/Online Learning and Meetings	Teams/Online Learning and Meetings section added	February 2021	L Askin
4.0	Acceptable Use	Guidance added on sharing screens	January 2023	L Askin
5.0	Acceptable Use	Guidance on use of dashcams	April 2023	L Askin
6.0	Acceptable Use	Work devices at home	November 2023	L Askin
7.0	Changed into an Online Safety policy incorporating Acceptable Use.	Updated for KCSIE changes re Online Safety	December 2023	IT Director
8.0	Appendices	Addition to section 6.4 as an appendix. This will be built into the main body of the policy when next reviewed.	January 2024	IT Director
9.0	Appendix 1,2 &3	Using applications or tools to secretly listen in on a lesson or meeting is not permitted. Messages or communications on work devices may be requested under a subject access request. All messages and communications will be professional and comply with Data Protection policies.	April 2024	IT Director

10.0		Password protect any personal information sent.		
11.0	Acceptable use Section 9	Update to use staff using work devices in and outside school – You must not download Trust data onto personal devices, including computers, mobile phones, or tablets. Personal data must not be stored on personal devices such as computers, mobile phones, or tablets. Using initials is acceptable if they are not identifiable. (If there is a suspected breach of this policy, your personal device may be included in a subject access request in accordance with Government guidance)	September 2024	B Clay – Executive Assistant
12.0	Acceptable use Section 9	Removed the reference to Intune as no longer used. Staff are not permitted to use their personal Apple IDs on work devices. All staff and visitors are required to take care of school owned devices.	July 2025	IT Director
13.0	Acceptable Use Appendix 1	Added expected professional appearance when on video calls	January 2026	IT Director

Contents

1. Aims

We aim to:

- ensure the online safety and wellbeing of our pupils and staff
- Provide education on how to use technology and online systems and resources safely
- Mitigate risks
- Identify, intervene, escalate and resolve any incidents.
- Ensure the implementation of the policy meets safeguarding needs of the schools and Trust

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

- **Content Risk** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact Risk** – 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 Risk** – 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 Risk** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

2. Legislation and guidance

This policy is based on:

- Department for Education's (DfE's) statutory, Keeping Children Safe in Education, and its advice on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Searching, screening and confiscation

- DfE's guidance on protecting children from radicalisation.

- Education Act 2011, in relation to powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate items on pupils' devices where they believe there is a 'good reason' to do so.

- National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Local Governing Board (LGB)

As this policy is related to Safeguarding which is a delegated responsibility from Trust Board The governing board will ensure that:

- they monitor this policy and hold the headteacher to account for its implementation;
- co-ordinate regular meetings with appropriate staff to discuss online safety;
- monitor online safety alert reports as provided by the designated safeguarding lead (DSL);
- online safety is an ongoing and interrelated theme in the safeguarding culture, education, training, and approach teaching about safeguarding and online safety, is adapted for age appropriateness, vulnerable children, victims of abuse or pupils with special educational needs and/or disabilities (SEND).

3.2 The Headteacher

The Headteacher is responsible for ensuring that

- staff understand this policy, and that it is being implemented consistently throughout the school.
- any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy.

3.3 The Designated Safeguarding Lead (DSL)

The DSL is responsible for ensuring that:

- the policy is understood and implemented consistently, with the Headteacher;
- they address any online safety issues or incidents with the Headteacher;
- all online safety issues and incidents are managed in line with the school child protection policy;
- online safety or cyber bullying incidents are recorded, reported, and dealt with appropriately in line with this policy;
- staff training on online safety is provided;
- they liaise with other agencies and/or external services as necessary;
- regular reports on online safety in school are provided to the Headteacher and/or local governing board;
- parents/carer are liaised with regularly to ensure they understand expectations.

3.4 Trust IT Director

The Trust IT Director is responsible for ensuring (along with the IT team) that:

- effective security protection procedures are in place, such as filtering and monitoring systems. This is to reduce the risk of potentially harmful and inappropriate content and contact online, including terrorist and extremist material;
- IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- full security checks and monitoring the school's IT systems ongoing throughout each day;
- systems are in place to blocking access to potentially dangerous sites and reduce the risk of downloading of dangerous files;
- all online safety incident alerts are dealt with appropriately in line with this policy.

3.5 All staff, Governors, Members and Trustees

All staff, Governors, Members and Trustees are responsible for:

- understanding and complying with this policy;
- working with the DSL to ensure that any online safety incidents or cyber-bullying incidents are recorded and dealt with appropriately in line with this policy;
- following the safeguarding policy in relation to reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

3.6 Parents, carers, and pupils

Parents or carers are expected to ensure their child has understood, agreed to, and implements the terms on the acceptable use policy.

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

- UK Safer Internet Centre
- Childnet International
- Parent/carer resource sheet – Childnet International

Pupils agree to and implement the terms of the acceptable use policy. There are two pupil acceptable use policies (primary and secondary).

3.7 Visitors, Volunteers, Contractors, Suppliers/Service Providers, Agency Staff, and members of the community

Any individual who uses the Trust IT systems or internet will be required to agree to the terms of the Trust's acceptable use policy.

There is an acceptable use policy for agency staff and for visitors (see appendices).

4. Educating pupils about online safety

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

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

Primary 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.

Secondary schools:

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 and 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 which 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)

All schools:

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's DSL will raise parents'/carers' awareness of internet safety in communications home, meetings and in information via our website and social media. This policy will be on the Trust website and the link will also be shared with parents and online safety communications are issued monthly.

If parents 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.

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/relationship 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.

Teaching staff are 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.

Training on cyber-bullying, its impact and ways to support pupils, is included on our mandatory safeguarding training (see section 11).

The school will provide information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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, and any member of staff authorised to do so by the headteacher (as set out in the school 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, the authorised staff member will:

- Assess how urgent the search is, and consider the risk to other pupils and staff
- 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 cooperation

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, the school response will be in line with the behaviour policy). 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 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
- School behaviour policy and searches and confiscation policy (where applicable)

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 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.

The Trust will treat any use of AI to bully pupils in line with schools' anti-bullying policies and behaviour/relationship policies.

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 or Trust.

7. Acceptable use of the internet

All users of Trust IT, Wi-Fi and networks are required to comply with and sign the Trust acceptable use policy (as relevant to their role). See Appendices for Acceptable Use Policies.

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 internet usage and websites visited to ensure compliance.

8. Pupils using mobile devices in school

The policy for the use of mobile phones in schools is set out in each schools' behaviour/relationship policy.

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

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

9. Staff using work devices in and outside school

All staff members will take appropriate steps to ensure their devices remain secure. All staff must comply with the acceptable policy.

We will ensure hard drives remains secure through the hard drive encryption. 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.

Keeping operating systems up to date by returning the device to IT, when requested, to ensure the latest updates are installed.

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

You must not download Trust data onto personal devices, including computers, mobile phones, or tablets.

Personal data must not be stored on personal devices such as computers, mobile phones, or tablets. Using initials is acceptable if they are not identifiable. (If there is a suspected breach of this policy, your personal device may be included in a subject access request in accordance with Government guidance.)

10. New IT Systems/Programme/Website

All staff will comply with the Trust finance policy and data protection policy prior to using a new IT system/programme/website. This will include a data protection impact assessment and due diligence and but approval for any new supplier.

11. How we 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 school behaviour 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 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 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 will receive training, as part of their safeguarding 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 (e.g., 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/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 DSD/DSDs 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 and Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

13. Monitoring arrangements

The DSL records behaviour and safeguarding issues related to online safety. The Headteacher, senior leadership team, DSL and Network Manager will perform an annual review of online safety (such as the one available here) and this will be reported on to the local governing board, Trust Executive Safeguarding Lead and Trustees.

The Headteacher and DSL will annually update an 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. This will be reported to the local governing board, the Trust Executive Safeguarding Lead and Trustees

The IT team and safeguarding team will perform an annual audit to ensure this policy is complied with.

We will review staffs understanding of this policy through a three-tied approach to monitor, evaluate and review effectiveness (as part of the overall review of safeguarding):

- School
- Sheffield Children's Safeguarding Partnership (SCSP)
- Learn Sheffield

Appendix 1 Staff Acceptable Use for Online Safety and Social Networking Standards

The Trust recognises that the use of ICT, Internet, SharePoint, the Learning Platform, and a wide range of electronic communication can greatly enhance the quality of learning across our Trust.

It is vital that everyone adheres to this policy to ensure safe, appropriate, and responsible use of such technologies.

Acceptable Use

- I will read and comply with the ***Trust's Data Protection Policy.***
- All data stored by staff is the property of the Trust and should not be removed when staff leave.
- I will not disclose my username or password to anyone.
- I will not write down or store a password insecurely.
- I will always log off the computer when I have finished and lock it when unattended on school owned and personal devices.

- I will never use anyone else's login, email address or password.
- When working away from school I will only log into school systems using a secure wi-fi network.
- I will not use my personal email or personal phone number as a contact for pupils.
- I will never use my personal email address for work.
- When communicating electronically with pupils or parents it will only be via the school's accredited systems.
- I will ensure that all communication is transparent and open to scrutiny.
- I understand that any messages or communications on work devices (laptops, phones, email, what's app, text etc) may be requested under a subject access request. All messages and communications will be professional and comply with Data Protection policies.
- I will ensure that communication with pupils is in a professional manner.
- I understand that the use of the network or any school device to knowingly access inappropriate materials is strictly forbidden and may constitute a criminal offence.
- I will report any accidental access to unacceptable material immediately to my manager and notify my manager if I suspect someone else of misusing ICT. I will also inform the Designated Safeguarding

  Lead if misuse may be a child protection issue.
- I will ensure that pupils under my supervision use ICT facilities and the Internet appropriately to support learning. I will challenge and report any misuse.
- Where I am sharing my screen with others (including whiteboards) I will ensure sensitive / personal data is not shared unintentionally. This can be achieved by using extended desktop or freezing a duplicated display.
- I will ensure the ICT team have screened all devices for malicious software before connecting to the network and take care when opening unknown email attachments. I will seek advice from the ICT team if I am unsure about the safety of any such devices or attachments.
- I will make sure that if I need to transport personal data of any kind, I will do so using an encrypted external device that has a password in line with the ***Trust's Data Protection Policy.***
- I will password protect any personal information that I send via email and send the password via another means, e.g. phone call or text message.

- I will not attach any devices to the network that may contain files that breach copyright, GDPR or other laws.
- I agree to use the school's ICT only for work related use during my directed working hours.
- If I use a work mobile device or laptop at home and in school, I will not access inappropriate applications/ Internet searches (including gambling).
- I will not share my work device with family or friends.
- I will take all reasonable steps to ensure the safety of ICT which I take off site and will remove anything of a personal nature before it is returned to school.
- My mobile device (phones, tablets, smart wear) will be turned off or kept on silent mode during working hours except if required to authenticate with school network login or email, or in an emergency with the agreement of a member of the Senior Leadership Team.
- Employees should not access personal emails or messages during directed working hours except in an emergency with the agreement of a member of the Senior Leadership Team.
- I will only photograph or video pupils on school devices as part of a planned learning activity or, in exceptional circumstances, for identification purposes and will ensure footage is only used with the correct consent.
- I will not photograph or video pupils on personal devices.

  If I choose to have my school email account configured on my personal mobile device, I will set a 6digit passcode.
- I understand that the Trust monitors Internet usage and sites used by staff. All inappropriate searches are automatically alerted to the DSL and Headteacher.
- I understand that the misuse of ICT facilities and the Internet could result in disciplinary action being taken.
- I will follow Trust password policy of: At least 8 characters, at least 1 capital letter, at least 1 number.
- When working from home I will not leave any school system logged in unattended, these include remote access, Bromcom, SharePoint and video conferencing meetings or training.
- If I have a dashcam fitted in my car I will ensure that any internal audio recording will be disabled if I am making or receiving work related calls. I will also disable any internal video (if applicable)/audio recording if I am transporting children between locations.

- Using applications or tools to secretly listen in on a lesson or meeting is not permitted.
- I will not use my personal Apple ID on a work device and will setup a work Apple ID linked to my School/Trust email account.
- All staff are responsible for ensuring that any IT equipment provided by the Trust is used with care and kept in good working condition. This includes handling devices responsibly, storing them securely, and reporting any faults, damage, or loss immediately to the IT team. Staff must not attempt to repair or modify equipment themselves. Any misuse, neglect, or failure to report issues may result in the user being held accountable for any resulting damage or security risks. By using Trust provided IT equipment, staff agree to take reasonable steps to protect and maintain it, ensuring its availability and functionality for educational and administrative purposes.

Online Learning and Meetings - including Teams and Zoom

To find out how to do any of the below please visit the Trust Knowledge Base site to access useful guides - https://tsat.sharepoint.com/sites/tsat/policies/KnowledgeBase

- When using Teams always blur your background when providing online lessons, recording online content, or attending a meeting when outside of school.
- When using Zoom for a meeting whilst outside of school always upload and apply a custom background.
- Only use scheduled meetings setup in your Teams/Zoom calendar with pupils or meeting attendees.
- Make sure you end the meeting when meeting with pupils (or meetings attendees) and do not just leave.
- Always set the lobby option to 'Only me' (organiser) in Teams and enable the Waiting Room in Zoom for all external meetings and lessons so that you know who is attending, and you can admit each person to the meeting.
- Always set the who can present option to 'Only me' (organiser) for all lessons with pupils. In Zoom you need to change the share screen advanced sharing options for who can share to 'Only Host' (organiser). Its optional whether you want to do this for meetings with adults in Teams/Zoom.

If recording a meeting, always make sure the attendees are aware and they are happy for you to record the meeting, if they are not then do not record. Once you start the recording state that the

meeting is being recorded and participants have consented to it. *"Please note that any attempt to covertly record such a meeting may be considered as gross misconduct".*

- When entering a meeting/lesson you should always seek to ensure that your camera and microphone is active so that the person leading the meeting/lesson is made aware of your presence.
- If there are any issues with the use of camera (i.e., WIFI or data issues) then you should make the person/s leading the meeting/lesson aware of this.
- Any use of message chat should be to appropriately contribute to the meeting/lesson taking place. It should be the person/s leading the meeting who decide if the message chat needs to be shared on the screen to support the meeting.
- Staff must ensure they are appropriately dressed for all video calls, maintaining the same standard of professional appearance expected when attending meetings in person.

Staff social networking standards

Below sets out the standards expected of all staff when using social media.

DO

- Always act responsibly. Even if you do not identify your profession or place of work, your conduct could jeopardise any professional registration and/or your employment.
- Be considerate to your colleagues. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual.

DO NOT

- Share confidential information online.
- Build or pursue relationships with pupils even when the pupil has left the Trust.
- Use social networking to inform professional practice without careful consideration and discussions with management.

- Discuss pupils, parents, colleagues, school, or Trust in a way which may be deemed inappropriate or damage reputation.
- Post pictures of pupils/families online even if they have asked you to do this.
- Take pictures of parents, carers, or pupils without the relevant consents.
  Raise concerns about your work online. If you have concerns, then these should be discussed with your line manager.
- Engage in activities online which may bring the Trust into disrepute.
- Be abusive, bully, derogatory, defamatory, or offensive.
- Employees may not use social networking sites or other unauthorised sites during directed working hours.

All the above applies to open and private sections of social networking sites.

Appendix 2 - Pupil Acceptable Use for Online Safety and Social Networking Standards

The Trust recognises that the use of IT, Internet, SharePoint, the Learning Platform, and a wide range of electronic communication can greatly enhance the quality of learning across our Trust.

It is vital that everyone adheres to this policy to ensure safe, appropriate, and responsible use of such technologies.

Here at the Trust, we want every pupil to embrace the use of IT, Internet, and a wide range of electronic communication to enhance learning. However, it is vital that every pupil fully understands and adheres to the required policy that ensures safe, appropriate, and responsible use of such technologies. The agreement set out in this document applies to any activity undertaken both in school and outside of school. Misuse of the IT system, Internet or any form of electronic communication will result in you being denied use of this provision as well as further sanctions. Please take time to read this agreement carefully and make sure you fully understand each point before signing the agreement.

Acceptable Use This applies to school devices and personal devices being used in school and school/Trust owned devices being used at home

I will:

- only access the school's IT systems and Internet via my own username and password.
- keep my password safe and not share it with other people.
- ask the IT team to check any attachments or links before I click on them if I don't know that they are safe.
- if given permission to use my own device in school ask the IT team to check the device I want to link to the school IT before I do it to make sure there are no viruses.
- follow guidelines for safe use of the Internet.
- report any materials or conduct which I feel is unacceptable to the Teacher or IT Team.
- only use my own device in school if I have permission.
- immediately report any IT damage or faults.

I will not

- damage school IT on purpose.
- download IT viruses on purpose.
- play computer games during the school day unless I have been directed to do so by a teacher.
- alter or delete another person's files.
- use chat rooms and social networking sites during the school day.

- put personal information on-line (this could include names, addresses, email, telephone numbers, age, gender, educational details, financial details etc).
- do anything online which is offensive, hurtful, or otherwise upsetting to another person.
- post anonymous messages or forward chain letters.
- use inappropriate language.
- take, publish, or share pictures or videos of anyone without their permission.
- use school IT for personal use without a teacher's permission.
  copy someone else's schoolwork and pretend it is my own.
- access inappropriate materials such as pornographic, racist, or offensive material.
- install or attempt to install or store programmes on any school device.
- try to alter computer settings.
- will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- use any programs or software that might allow me to bypass the filtering/security systems.
- use applications or tools to secretly listen in on a lesson or meeting.

I understand that

- school will monitor my use of the systems, devices, and digital communications. School may share this information with my parents/carers, the police or other agencies depending upon the severity of the incident. School may check my school documents for viruses and unsuitable material at any time.
- if I use my own devices in the school, I will follow the rules set out in this agreement.
- I am responsible for my actions, both in and out of school.
- the school also has the right to act against me if I am involved in an incident out of school (examples would be cyber-bullying, use of images or personal information).

I have read and understood the above statements and I agree to the rules for use of ICT facilities and the Internet. I understand that deliberate failure to do this could result in the loss of my access rights to IT along with further sanctions if there was serious misuse.

Pupil signature.....Form Group.....

Pupil full name.....Date.....

This agreement will be re-issued annually, and access to systems will be revoked unless this is returned to the school.

Appendix 3 - Supply Staff Acceptable Use for Online Safety and Social Networking Standards

The Trust recognises that the use of ICT, Internet, SharePoint, the Learning Platform, and a wide range of electronic communication can greatly enhance the quality of learning across our Trust.

It is vital that everyone adheres to this policy to ensure safe, appropriate, and responsible use of such technologies.

Acceptable Use

- I confirm that I have received **Data Protection Training** within the last year and I / or my supply agency have provided evidence of this to the Trust.
- I confirm that I have read, understand, and agree to comply with the **Supply staff pack**.
- I will not disclose my username or password to anyone.
- I will not write down or store a password insecurely.
- I will always log off the computer when I have finished and lock it when unattended.
- I will never use anyone else's login, email address or password.
- I will not use my personal email or personal phone number as a contact for pupils.
- I will never use my personal email address for work.
- When communicating electronically with pupils or parents it will only be via the school's accredited systems.
- I will ensure that all communication is transparent and open to scrutiny.
- I will ensure that communication with pupils is in a professional manner.
- I understand that the use of the network or any school device to knowingly access inappropriate materials is strictly forbidden and may constitute a criminal offence.
- I will report any accidental access to unacceptable material immediately to the headteacher and notify the headteacher if I suspect someone else of misusing ICT. I will also inform the Designated Safeguarding Lead if misuse may be a child protection issue.
- I will ensure that pupils under my supervision use ICT facilities and the Internet appropriately to support learning. I will challenge and report any misuse.

Where I am sharing my screen with others (including whiteboards) I will ensure sensitive / personal data is not shared unintentionally. This can be achieved by using extended desktop or freezing a duplicated display.

- I will ensure the ICT team have screened all devices for malicious software before connecting to the network and take care when opening unknown email attachments. I will seek advice from the ICT team if I am unsure about the safety of any such devices or attachments.
- I will not attach any devices to the network that may contain files that breach copyright, GDPR or other laws.
- I agree to use the school's ICT only for work related use during my directed working hours.
- My mobile device (phones, tablets, smart wear) will be turned off or kept on silent mode during work except if required to authenticate with school network login or email, or in an emergency with the agreement of a member of the Senior Leadership Team.
- I will not access personal emails or messages during directed working hours except in an emergency with the agreement of a member of the Senior Leadership Team.
- I will only photograph or video pupils on school devices as part of a planned learning activity or, in exceptional circumstances, for identification purposes and will ensure footage is only used with the correct consent.
- I will not photograph or video pupils on personal devices.
- I understand that the Trust monitors Internet usage and sites used by staff. All inappropriate searches are automatically alerted to the DSL and Headteacher.
- I understand that the misuse of ICT facilities and the Internet could result in disciplinary action being taken.
- All data stored by supply staff is the property of the Trust and should not be removed when staff leave.
- If I have a dashcam fitted in my car I will ensure that any internal audio recording will be disabled if I am making or receiving work related calls. I will also disable any internal video (if applicable) / audio recording if I am transporting children between locations.
- I understand that any messages or communications on work devices (laptops, phones, email, what's app, text etc) may be requested under a subject access request. All messages and communications will be professional and comply with Data Protection policy.

- I will password protect any personal information that I send via email and send the password via another means, e.g., phone call or text message.
- All supply staff are responsible for ensuring that any IT equipment provided by the Trust is used with care and kept in good working condition. This includes handling devices responsibly, storing them securely, and reporting any faults, damage, or loss immediately to the IT team. Supply staff must not attempt to repair or modify equipment themselves. Any misuse, neglect, or failure to report issues may result in the user being held accountable for any resulting damage or security risks. By using Trust provided IT equipment, supply staff agree to take reasonable steps to protect and maintain it, ensuring its availability and functionality for educational and administrative purposes.

Staff social networking standards

Below sets out the standards expected of all staff when using social media.

DO

- Always act responsibly. Even if you do not identify your profession or place of work, your conduct could jeopardise any professional registration and/or your employment.
- Be considerate to your colleagues. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual.

DO NOT

- Share confidential information online.
- Build or pursue relationships with pupils even when the pupil has left the Trust.
- Use social networking to inform professional practice without careful consideration and discussions with management.
- Discuss pupils, parents, colleagues, school, or Trust in a way which may be deemed inappropriate or damage reputation.
- Post pictures of pupils/families online even if they have asked you to do this.
- Take pictures of parents, carers, or pupils without the relevant consents.

- Raise concerns about your work online. If you have concerns, then these should be discussed with the Headteacher.
- Engage in activities online which may bring the Trust into disrepute.
- Be abusive, bully, derogatory, defamatory, or offensive.
- Supply staff may not use social networking sites or other unauthorised sites during directed working hours.

All the above applies to open and private sections of social networking sites.

Full name ……

Signature ……

Date ……

Appendix 4 Visitor Acceptable Use Policy

The Trust recognises that the use of ICT, Internet, SharePoint, the Learning Platform, and a wide range of electronic communication can greatly enhance the quality of learning across our Trust.

It is vital that everyone adheres to this policy to ensure safe, appropriate, and responsible use of such technologies.

This policy is for visitors who log on to school guest networks.

Acceptable Use

- I will not write down or share the guest wireless password. I understand that use of the network to knowingly access inappropriate materials is strictly forbidden and may constitute a criminal offence.

- I will report any accidental access to unacceptable material immediately to the headteacher and notify the headteacher if I suspect someone else of misusing ICT if misuse may be a child protection issue.

- My mobile devices will be turned off or kept in silent mode whilst in school except in an emergency with the agreement of the headteacher.

- I will not photograph or video pupils unless agreed with the headteacher in advance, to ensure consent is obtained.

- I understand that the Trust monitors internet usage and sites used by visitors who are connected to the school's network. All inappropriate searches are automatically alerted to the Designated Safeguarding Lead (DSL) and headteacher.

- I understand that the misuse of ICT facilities and the internet could result in the headteacher being informed to review if there is a safeguarding risk to staff or pupils.

- All visitors are responsible for ensuring that any IT equipment provided by the Trust is used with care and kept in good working condition. This includes handling devices responsibly, storing them securely, and reporting any faults, damage, or loss immediately to the IT team. Visitors must not attempt to repair or modify equipment themselves. Any misuse, neglect, or failure to report issues may result in the user being held accountable for any resulting damage or security risks. By using Trust provided IT equipment, visitors agree to take reasonable steps to protect and maintain it, ensuring its availability and functionality for educational and administrative purposes.

Addendum

Addition to section 6.4: Artificial Intelligence (AI).

- Creating or sharing deepfake pornography of someone without their permission is a new criminal offence under the Online Safety Act 2023. Find out what the act means for your school, as well as a list of the new and revised offences.