

Online Safety Policy (E-Safety)



| | | |
|---------------------|---|---|
| Approved by: | Penny Harris (Director) Jane Cox (Director) Steven Pryer (IT Manager) | Date: 19 th November 2024 |
|---------------------|---|---|

| | |
|--------------------------|------------------------------|
| Last reviewed on: | 5 th October 2023 |
|--------------------------|------------------------------|

| | |
|----------------------------|--------------------------------|
| Next review due by: | 1 st September 2025 |
|----------------------------|--------------------------------|

All policies are generated and reviewed with an awareness of equality and diversity in relation to pupils, staff and visitors. All policies are generated placing safeguarding and wellbeing at the heart of all that we do.

Contents

| | |
|--|----|
| 1. Aims | 2 |
| 2. Legislation and guidance..... | 3 |
| 3. Roles and responsibilities | 3 |
| 4. Educating pupils about online safety | 6 |
| 5. Educating parents/carers about online safety | 8 |
| 6. Remote Learning..... | 8 |
| 7. Cyber-bullying | 8 |
| 8. Artificial intelligence (AI)..... | 10 |
| 9. Acceptable use of the internet in school | 10 |
| 10. Pupils using mobile devices in school | 11 |
| 11. Staff using work devices outside school | 11 |
| 12. How the school will respond to issues of misuse | 11 |
| 13. Training | 11 |
| 14. Monitoring arrangements..... | 12 |
| 15. Links with other policies | 12 |
| Appendix 1: Acceptable use agreement (pupils) | 13 |
| Appendix 2: Acceptable use agreement (Parents and Carers) | 14 |
| Appendix 3: Acceptable use agreement (staff, directors, volunteers and visitors) | 15 |
| Appendix 4: Online safety training needs – self-audit for staff | 16 |
| Appendix 5: Online safety incident report log | 17 |
| Appendix 6: Online Safety Risks..... | 17 |
| Cyberbullying | 17 |
| Online grooming | 18 |

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and directors
- 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 head teachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE’s guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

3. Roles and responsibilities

3.1 The directors

The directors have overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The directors 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 directors 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 directors will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs.

The directors will ensure children are taught how to keep themselves and others safe, including keeping safe online.

The directors will 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 the 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 directors 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 approach to safeguarding and related 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 head teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. The head teacher will also ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) 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 head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Online Safety Lead and IT manager to make sure the appropriate systems and processes are in place
- Working with the Online Safety Lead, Senior Leadership Team 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 and safeguarding policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this and the Behaviour Management policy
- Managing online safety issues in line with the school child protection 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 head teacher and directorial 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 IT manager

The IT manager 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 termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 (appendix 1)
- 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
- Working with the DSL to ensure that online safety incidents and cyber-bullying incidents are dealt with appropriately
- Ensuring that any online safety incidents are logged and working with the DSL to ensure they are 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 Management 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.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Read, understand and agree to the terms on acceptable use of the school's ICT systems and internet (appendix 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](#)

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

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 Key Stage 2**, 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 that 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. The school will use group work opportunities to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this. 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' awareness of internet safety in direct communications and via information on our website. This policy will also be shared with parents.

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

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

6. Remote Learning

6.1 Responsibilities

The directors are responsible for monitoring the school's approach to providing remote learning to ensure education remains as high quality and safe as possible. The SLT and subject leads are responsible for considering whether any aspects of the subject curriculum need to change to accommodate remote learning. SLT and subject leads are responsible for working with teachers who are teaching remotely to ensure all work set is appropriate and consistent. SLT and subject leads are responsible for monitoring the remote work set by teachers. Teachers are responsible for continuing to set work for each pupil they are timetabled to teach. Teachers must be available on Google Classroom for the duration of each timetabled lesson. Teachers must provide feedback to pupils during each timetabled session. Teachers must record all attendance in lessons on Google Classroom. Teachers must record all communication with parents on a contact form. Teachers must record any concerns on a concern form. Communication with pupils and parents must only take place during school hours. The Designated Safeguarding Lead is responsible for child protection and wider safeguarding in relation to remote learning

6.2 IT Issues and Safeguarding

A staff member is allocated to help staff, parents and pupils with any technical issues they are experiencing during remote learning. Teachers will only use school equipment to deliver remote learning and not share these devices with family or friends.

7. Cyber-bullying

7.1 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 Anti Bullying policy.)

7.2 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.

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, directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 13 for more detail).

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 head teacher 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.

7.3 Examining electronic devices

The head teacher, and any member of staff authorised to do so by the head teacher (as set out in the Behaviour Management 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 head teacher 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, head teacher, or another 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](#)
- Our Behaviour Management 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.

8. 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.

On Track Education 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.

On Track Education will treat any use of AI to bully pupils in line with our Anti Bullying 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 On Track Education.

9. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and directors 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, directors 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.

10. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but may be required to hand them in for secure keeping during the school day. Mobile phones must not be used in lessons.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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.

11. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

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

Work devices must be used solely for work activities. Work devices must not be shared with family or friends.

12. How the school will respond to issues of misuse

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

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

13. 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:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh 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 will undertake child protection training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

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

14. Monitoring arrangements

The DSL, head teacher and directors monitor incident logs and safeguarding issues related to online safety.

This policy will be reviewed annually by the directors and head teacher.

15. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Management Policy
- Staff Code of Conduct Policy
- Staff Disciplinary Policy
- Data Protection and GDPR Policy
- Complaints Policy

Appendix 1: Acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a staff member being present, or without a staff member's permission
- Access any inappropriate websites
- Access social networking sites (unless a staff member 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 member of staff
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of a staff member or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

When remote learning from home using live streaming, I will:

- Use appropriate language
- Wear appropriate clothing
- Behave appropriately
- Take care of school IT equipment
- Not record or take still photos of online lessons

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand it in for secure safekeeping during the school day, on request
- I will not use it during lessons without a staff member's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit.

I will immediately let a 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.

Signed (pupil):

Date:

Appendix 2: Acceptable use agreement (Parents and Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS AND CARERS

Name of pupil:

When using the school's ICT systems and accessing the internet in school, my child will not:

- Use them for a non-educational purpose
- Use them without a staff member being present, or without a staff member's permission
- Access any inappropriate websites
- Access social networking sites (unless a staff member 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 member of staff
- Use any inappropriate language when communicating online, including in emails
- Share their password with others or log in to the school's network using someone else's details
- Give their personal information (including name, address or telephone number) to anyone without the permission of a staff member or parent/carer
- Arrange to meet anyone offline without first consulting their parent/carer, or without adult supervision

When remote learning from home using live streaming, I will make sure my child:

- Uses appropriate language
- Wears appropriate clothing
- Behaves appropriately
- Takes care of school IT equipment
- Does not record or take still photos of online lessons

If my child brings in a personal mobile phone or other personal electronic device into school, this may be handed in. I agree that the school will monitor the websites my child visits. I will immediately let a member of staff know if my child finds any material which might upset, distress or harm them or others.

Parent/ Care 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 in the pupil's agreement on using the school's ICT systems and internet, and I will make sure my child understands these.

If my child is given use of school equipment at home, I will make sure that:

- Their login is not shared
- It is used for school purposes only
- The machine will be taken care of

Signed by Parent/Carer:

Date:

Appendix 3: Acceptable use agreement (staff, directors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, DIRECTORS, VOLUNTEERS AND VISITORS

Name of staff member/director/volunteer/visitor:

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- 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
- 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

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

I agree that the school will monitor the websites I visit.

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) / E-Safety lead / head teacher know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

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

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

Date:

Appendix 4: Online safety training needs – 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, directors and visitors? | |
| 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 5: Online Safety Risks

We have to accept that we cannot completely monitor material held by pupils on mobile phones, tablets, etc, but we can ensure that sufficient information is given to students to allow them to make good decisions and help them to keep themselves safe. It is also the case that this is a very fast moving range of technologies and policies and procedures can

be out of date almost as soon as they are written. We are also mindful that many students have greater knowledge than some staff in managing new technologies.

Broadly, online safety falls into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful materials

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

Cyberbullying

Cyberbullying can take the following forms:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or video.
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding from online games, activities or friendship groups
- setting up hate sites or groups about a particular person
- encouraging to [self-harm](#)
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages
- sharing of nudes or semi-nudes
- pressuring into sending sexual images or engaging in sexual conversations.

The sharing of nudes or semi-nudes is when sexually explicit photos or messages are sent to other people's mobile phones. These photos/messages can then be forwarded and seen by many people, causing embarrassment and long term effects such as depression and anxiety.

It is a crime to send a sexually explicit photo to another person and under 18s can be charged with possessing and distributing child pornography. They can also be put on the sex offenders register.

The UKCCIS (UK Council for Child Internet Safety) Guidance: Sexting in schools and colleges, responding to incidents, and safeguarding young people (2017) will be followed by all staff.

Online grooming

Grooming is when someone builds an emotional connection with a young person to gain their trust for the purposes of sexual abuse, exploitation or radicalisation. Groomers may be male or female and they could be of any age. Many young people do not understand that they have been groomed, or that what has happened has been abuse. Groomers can use social media sites, instant messaging apps or online gaming platforms to connect to a young person. They can spend time learning about a young person's interests from on-line profiles and then use this knowledge to help them build a relationship. It is easy for groomers to hide their identity on-line. They may pretend to be another young person and then chat and become 'friends' with the young person they are targeting.

Groomers may look for:

- Usernames that are flirtatious or have a sexual meaning
- Public comments that suggest a young person has low self-esteem or is vulnerable

Increasingly, groomers are sexually exploiting their victims by persuading them to take part in on-line sexual activity

Information and support

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

www.educateagainsthate.com