HOVINGHAM PRIMARY SCHOOL

01/09/2022

Online Safety Policy

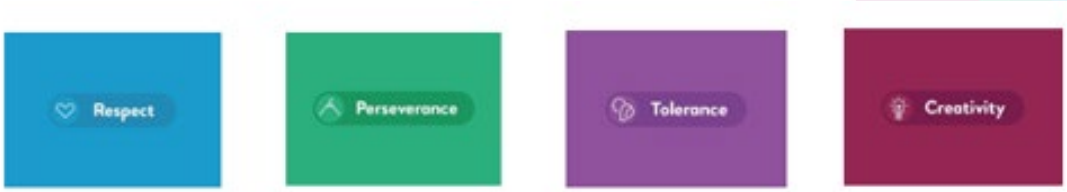
Hovingham Primary School

Online Safety Policy

Date: September 2022
Review date: September 2023

Aims

At Hovingham Primary School, we are motivated by our purpose to give our children the best experiences we our aim is to be a great school where everyone aims high and we do this through our Core Values:



It is these values which underpin our high expectations for behaviour within school.

At Hovingham Primary School we want to keep all children safe when using technology, this includes the use of mobile devices such as tablets. We want to teach children the correct procedures to follow if they come across something that they should not see or upsets them when working with technology.
At Hovingham we believe that children have the right to enjoy their childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own and other's online behaviour and develop effective strategies for staying safe and making a positive contribution online. This policy describes the knowledge, understanding and skills that children and young people should develop through their time at Hovingham.

We aim to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers, and Governors

• 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

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 Headteachers/ Heads of School and school staff
- Relationships and sex education
- Searching, screening and confiscation

It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

The policy also considers the National Curriculum computing programmes of study, Hovingham's Personal Development approach and Hovingham's safeguarding curriculum.

This policy should be read in conjunction with:

- Behaviour Policy
- Complaints Procedure
- Data Protection Policy and privacy notes
- ICT and Internet Acceptable Use Policy
- Safeguarding and Child Protection Policy
- Complaints Procedure

Roles and responsibilities

The Principal or, in her absence, the Vice Principal, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care. The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Governors will:	• The governing body will monitor, develop and review the policy and its implementation in school. • There is a named link governor (????????) for computing and online safety who works closely with, and in support of, the lead member of staff. • When aspects of computing and online safety appear in the School Improvement Plan, a governor will be assigned to reflect on, monitor and review the work as appropriate.
Principal will:	• Ensuring that staff understand this policy and that it is being implemented consistently throughout the school • Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents • Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy • Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy • Updating, organising and delivering staff training on online safety • Liaising with other agencies and/or external services if necessary
DSLs will:	• Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 regular basis • Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially

	dangerous files
The safeguarding team will:	• Discuss any concerns at weekly safeguarding meetings where we discuss 'who we are worried about'. • This additional support might involve: ▪ further monitoring ▪ working with an outside agency ▪ providing some bespoke online safety work ▪ creating links with the family to provide additional support
The computing lead will:	• Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum • Work closely with the DSL and all other staff to ensure an understanding of the computing curriculum. • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements, including remote learning agreements. • Ensure the curriculum content is covered. • Monitor the impact of the curriculum. • Capture pupil voice and use this to review curriculum.
The PSHE lead will:	• Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ Relationships Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. • Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
All staff will:	• Maintaining an understanding of this policy • Implementing this policy consistently • Working with the DSL to ensure that any online safety incidents are logged 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 • Report any concerns to a DSL and record on the weekly WAWA.
Parents/ Carers will:	• Ensure they are aware of this policy. • Work with the school to keep their child safe online. • Monitor their child's online usage at home. • Report any online safety concerns to a DSL.

	Please see below for further information.

Educating and supporting parents with online safety

Hovingham will raise parents' awareness of internet safety, through usual forms of communication other communications home and through internet safety week. This policy will also be shared with parents, via the website and will inform parents:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Class teacher / strategic lead who will share with the DSL.

Curriculum Overview (computing and online safety)

The internet is an essential element for education, business and social interaction. The school offers provision to pupils to access the internet as part of their learning experience. It is also a resource for both staff and pupils. The text below is taken from the National Curriculum computing programmes of study.

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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

As part of the new Relationship Education and Health Education, pupils will learn:

Relationships Education (RE) links – Online relationships

- That people behave sometimes behave differently online. Including by pretending to be someone that 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 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.

Relationships Education (RE) links – Respectful Relationships

- About different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help.

Relationships Education (RE) links – Being Safe

- What sort of boundaries are appropriate in friendships with peers and others (including a digital context)
- How to respond safely and appropriately to adults that they might encounter (in all contexts, including online) whom they do not know.

Health Education links (HE) – Mental wellbeing

- That bullying (including cyber –bullying) has a negative and often lasting impact on mental wellbeing.

Definition of Cyber-bullying

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 Hovingham's Behaviour Policy.)

How do we prevent and address cyber-bullying

At Hovingham, all staff are advised to maintain an attitude of 'it could happen here' where safeguarding is concerned. When concerned about the welfare of a child, staff should always act in the best interests of the child.

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. This will be covered through:

- Computing curriculum
- Safeguarding curriculum
- PSHE curriculum (see Personal Development policy)
- Assemblies

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the behaviour code of conduct. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Please see the behaviour code of conduct for further information.

We will ensure that children know how they can report any incidents and are encouraged to do so.

As part of our personal development culture, we will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff and Governors will receive training on cyber-bullying, its impact and ways to support children, this is as part of safeguarding training (

We will also send regular information/leaflets 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 Behaviour Policy. Where illegal, inappropriate, or harmful material has been spread among our community, 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.

Health Education links (HE) – Internet safety and harms

- That for most people the internet is an integral part of life and has many benefits.
- About the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Why social media, some computer games, and online gaming, for example are age restricted.

- That the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- How to be a discerning consumer of information online including understanding that information from search engines, is ranked, selected and targeted.
- Where and how to report concerns and get support with issues online.

Please see the Living and Growing policy for further information.

Computing Policy - Further guidance and support is outlined in the Computing Policy, around subject intent, implementation and impact. There are also detailed Long Term and Medium Term plans to support teacher's short term planning.

Safeguarding and Child Protection

Online safety plays a very important part in fulfilling the statutory duties all schools have to meet and the online safety policy should be closely aligned to the school's safeguarding policy. Our computing / online safety curriculum helps pupils to know and understand how to keep themselves and others safe, make informed decisions and manage risk and equips them with the knowledge and skills to get help if they need it. When teaching any sensitive issue, pupils may give cause for concern, and a link needs to be made with the safeguarding team. All adults involved in the computing / online safety curriculum delivery need to be aware of the safeguarding arrangements in place.

Early Identification

To ensure early identification, weekly safeguarding meetings will be held where we discuss 'who we are worried about'. During this meeting, we will discuss any key children who have been identified by teachers and a plan will be put into place of what support we can offer these children within school. This additional support might involve:

- further monitoring
- working with an outside agency
- providing some bespoke online safety work
- creating links with the family to provide additional support

Parents will be informed of any additional support that is put in place.

Safeguarding within the curriculum

Within our safeguarding curriculum, we have an Y6 'Safety outside of Hovingham' module. This includes topics on:

- Grooming (Alright Charlie resources)
- Sexual Online Bullying (Just a Joke resources)

Please speak to the PSHE lead for further information on these topics.

Pupil Voice

Formal Pupil Voice

We often use online technologies to collect pupil voice (such as MHMS etc.). This is always completed under supervision, and results are always analysed within 24 hours to check for any safeguarding concerns. These will be passed onto a DSL immediately.

Informal Pupil Voice

As part of our school culture, we continually capture informal pupil voice through discussions, questionnaires and use these to inform our curriculum. Any issues / concerns identified, will be passed onto the computing lead / Personal Development lead / safeguarding team, who will put a plan into action.

Educating and supporting parents with online safety

The school recognises the key role that parents/carers fulfil in supporting their children with online safety outside of Hovingham. Therefore, we seek to work in partnership with parents/carers when planning and delivering our computing and online safety curriculum.

At Hovingham we will raise parents' awareness of internet safety, through usual forms of communication other communications home and through internet safety week.

The school will publish this policy information/leaflets on the school website about online safety to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Class teacher / strategic lead who will share with the DSL.

The school will encourage this partnership by:

- gathering parent /carers' views on the policy and take these into account when it is being reviewed
- providing access to resources and information being used in class and do everything to ensure that parents/carers are comfortable with the education provided to their children in school
- providing parents / carers with key information around online safety, and how they can best support at home
- expecting parents/carers to share the responsibility of online safety and support their children
- encouraging parents/carers to create an open home environment where pupils can engage, discuss and continue to learn about online safety

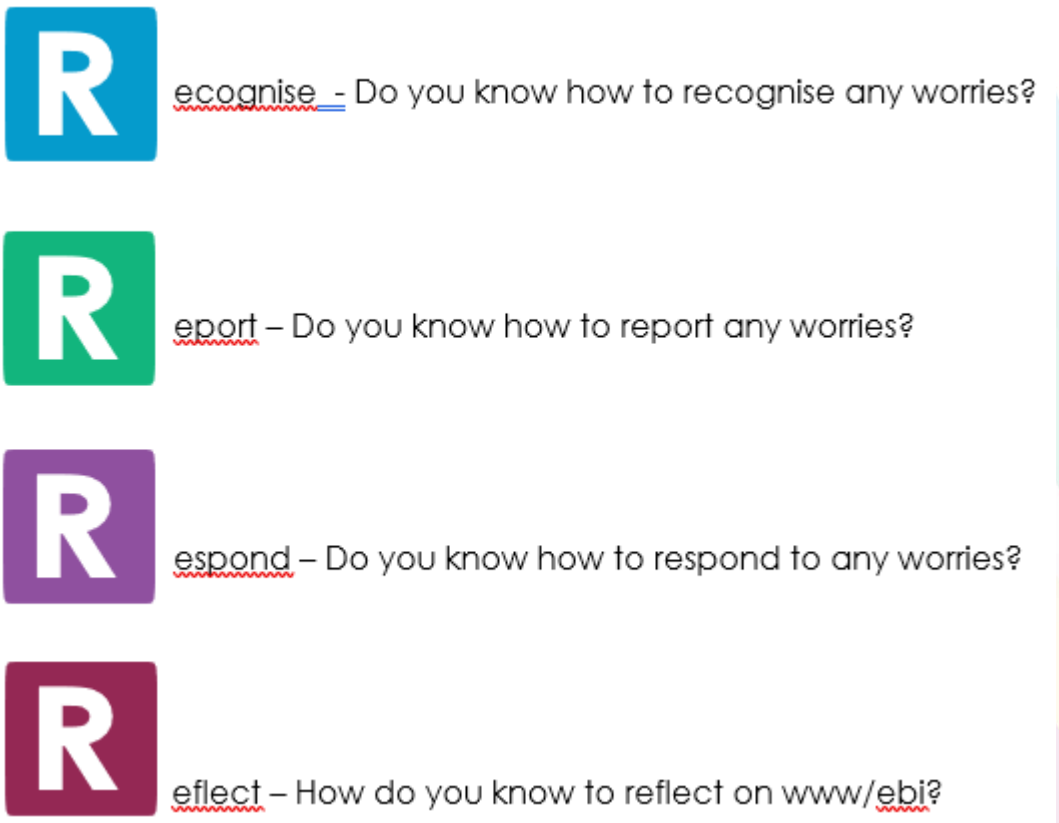
- providing support and encourage parents/carers to seek additional support in this from the school where they feel it is needed

The school will publish information/leaflets on the school website about online safety to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

How to report a concern:

Please follow the safeguarding procedure in school and speak to a DSL.

We follow the



<u>Managing Internet Safety</u>

Information system security

School ICT systems capacity and security are reviewed regularly. All internet access is filtered by the school's ISP (Internet Service Provider) and we will work together with them to ensure the efficacy of the filter as far as practicably possible. We recognise that no filter can ever be perfect, therefore, children will be taught the necessary skills to manage risks themselves on an age appropriate level.
Virus protection is updated continuously and a full scan is run daily.

Published content and the school website
The contact details on the school website should only include the school's e-mail address, address and telephone number. Staff e-mail addresses will not be published. The Principle will take overall responsibility for checking the accuracy and appropriateness of the content of the website.

Publishing pupils' images and work
Written permission will be obtained from Parents/Carers on entry, before photographs of children are placed up on the school website or any social media.
Pupil's full names will not be used on the school website, particularly in association with photographs.
• The School Network blocks/filters access from most social networking sites. Despite this, we will educate children on the safe use of these technologies as we are aware that our learners may choose to access these resources outside of school.
• Newsgroups are blocked unless a specific use is approved.
• Pupils will be advised never to give out any personal details which may identify them or their location.
• Pupils and parents will be advised that use of social networking sites outside of school is inappropriate for primary aged pupils, and further information will be provided to parents regarding this.

Managing Filtering
The school will work with Schools Broadband (or any future ISP) to ensure that systems to protect pupils are reviewed and improved. The school internet is subject to a filtering system called 'Smoothwall'.

If staff or pupils discover an inappropriate website it must be reported to the designated safeguarding lead. DSLs, will ensure that regular checks are made to ensure that the filtering methods selected are effective, appropriate and reasonable. Safeguarding breaches will be responded to through a sense check.

Where a staff member misuses the school's ICT system 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.

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

Managing emerging technologies
• Emerging technologies will be examined for educational benefit and children will be supervised and monitored when using these.
• Mobile phones are not to be used during school hours. The sending of abusive or inappropriate text messages is strictly forbidden. Pupils must not bring mobile phones or

smart watches into school and if they do, they must be switched off and stored securely in the school office until the end of the school day.
• Children will be educated about the risks inherent in the use of social messaging apps as we are aware that they may use these when outside of school.
• Staff will be issued with a school phone if contact with pupils or parents is required.

Managing data security
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2018.

Policy decisions

• All staff and governors must read and sign the 'Acceptable Use Policy' before using any school ICT resource.

• The school will keep a record of all staff/pupils who are denied internet access. The record will be kept up to date.

• In Key Stage 1, access to the internet will be under supervision, with access to approved online materials. In Key Stage 2, pupils will be supervised when accessing the internet.

• Parents will be asked to sign and return a consent form on their child's behalf when starting school to enable children to access the internet in school, this will outline the need to remain safe online and follow schools acceptable use policy.

- Whole class acceptable use policies signed.

Assessing risks

The school will take all reasonable precautions to ensure that users only access appropriate material.
However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Schools Broadband can accept liability for the material accessed, or any consequences of Internet access. Methods to identify, assess and minimise risks will be reviewed regularly. The school will audit ICT provision to ensure that its content is appropriate and its implementation effective.

Handling Online safety complaints

• Complaints of internet misuse and/or online safety will be dealt with by the school's designated safeguarding lead.
• Any complaint over staff misuse should be referred to the Principal or a DSL.
• Complaints of a child protection nature will be dealt with in accordance to school child protection procedures.
• Responses to internet misuse will include informing parents/carers of the incident.

• Further sanctions may include the removal of internet/computer access for a period of time.

Useful resources for staff

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com