Online Safety Policy

(Pupils, staff, parents, governors, visitors)

Academic Year 2021 - 22

High expectations
Caring
Positive attitudes
Successful

Policy Developed: October 2021
Policy approved:
Next review: September 2022

High expectations, Caring, Positive Attitudes and Successful

STRENGTHS OF OUR SCHOOL

The Children

Are well behaved, calm and polite
Are engaged, positive and resilient
Are supportive and helpful towards others
Have an input on important decisions
Have a sense of belonging

The Community

School supports the whole family not just the child
Recognises the importance of attendance
Spreads our growing reputation as a good school
Helps celebrate the children's achievements
Supports the school on improving behaviour

The Curriculum

Is a fun curriculum that is engaging
Maintains a strong focus on the basic skills
Is enriched through extra-curricular activities
Supports our most vulnerable children
Provides a rich variety of experiences & opportunities

The Staff

Develop nurturing relationships with children
Provide good quality teaching and learning
Support one another to help the children
Are consistent in how they treat children
Identify children's SEN needs early

THE CURRICULUM WE HOPE TO PROVIDE

Skills

Fluent and confident in Reading, Writing and Maths
Communicate with confidence
ICT skills fit for the future
Life skills – money, time, cooking
Safety skills – Swimming, healthy choices
Problem solving skills – Patience & Resilience

Attitudes

Confident and independent
The belief they can reach for the stars
Celebrate a range of cultures
Take responsibility for the environment
Be honest and learn from their mistakes
Children who are caring and helpful

Experiences

To have 1st hand experiences of…
Going away on a residential trip
Visiting a range of places of worship
A chance to look after an animal
Relevant trips to theatres/farms/beaches
Taking part in public performances
Work experiences & further education

Knowledge

High school ready English & maths
To know about local places of interest
To know where we are in the world
Life skills – money, time, cooking
Information about possible careers
To know major historical facts
To know their own strengths

Scope of the Policy

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, iPads, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Hunslet Carr Primary School, we recognise that learning is a lifelong process and that e learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities that are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy applies to all stakeholders of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but which are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

1. Aims

Our school aims to:

● Have robust processes in place to ensure the online safety of pupils, 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

● Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 governing board

Governors monitoring of the policy will be supported by governor visits and link governor reports.
The schools safeguarding governor is **Paul Wray**.

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.

3.3 The designated safeguarding lead (DSL)

The headteacher will ensure that our school has sufficient and appropriately trained staff in a Designated Safeguarding Lead (DSL) role.

Martin Lumb (Headteacher) has overall DSL responsibility for the school, with day-to-day responsibly for this delegated to **Andy Hinchcliffe** (Lead Child Protection Officer).
Details of our school's DSL's and deputy/deputies are set out in the Safeguarding and Child Protection policy as well as the staff handbook.

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

● Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

● Working with the Headteacher, ICT support provider (Primary ICT) and other staff, as necessary, to address any online safety issues or incidents

● Ensuring that any online safety incidents are logged (On CPOMS) and dealt with appropriately in line with this policy

● Ensuring that any incidents of cyber-bullying are logged (On CPOMS) and dealt with appropriately in line with the school's Anti-Bullying policy

● Updating and delivering staff training on online safety

● Liaising with other agencies and/or external services if necessary

● Providing regular reports on online safety in schools to the headteacher and governing board

This list is not intended to be exhaustive.

3.4 The ICT Support Provider

The ICT support provider (Primary ICT) is responsible for:

● Putting in place appropriate filtering (Smoothwall) 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

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, and ensuring that pupils follow the school's classroom rules on E-Safety (appendix 1)

● 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's Anti-Bullying Policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

● Notify a member of staff or the headteacher of any concerns or queries regarding this policy

● Ensure their child has read, understood and agreed to the classroom rules on acceptable use of the school's ICT systems and internet (appendix 1)

Parents 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 International

● Parent factsheet - Childnet International

● Healthy relationships – Disrespect Nobody

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 in the staff handbook.

4. Educating pupils about online safety

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

● Relationships education and health education in 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

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in communications home, and in information via our website and newsletters. This policy will also be shared with parents.

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.

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

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Anti-Bullying policy)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends 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's Anti-Bullying 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

As a general rule, school staff **will not** view any images on a pupil's electronic devices in case they are of an illegal nature.

In exceptional circumstances school staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

This would over ever take place with authorisation from the senior leadership team, after thorough consultation with the Education Safeguarding Team.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to agree to the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

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

8. Pupils using mobile devices in school

At Hunslet Carr Primary School we recognise that pupils and parents see that having access to a mobile phone is part of modern life and has become an essential way in which parents and carers can keep in touch with pupils on the way to and from school. It is important however that the use of the phone does not interfere with learning or cause a distraction or disruption to school life. As a result of this, we expect that all pupils bringing a mobile phone to school, hand it in to their class teacher at the start of the day and have it returned to them before leaving.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

● Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

● Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

● Making sure the device locks if left inactive for a period of time

● Not sharing the device among family or friends

● Installing anti-virus and anti-spyware software

● Keeping operating systems up to date – always install the latest updates

● Securely storing school devices at all times and not leaving any devices in an unsecure location (e.g. in a car)

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the Acceptable Use Policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from to the ICT Support Provider.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Acceptable Use 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 disciplinary procedures. 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.

11. Training

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

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

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

12. Monitoring arrangements

All incidents of online safety are logged via the CPOMS system in line with all safeguarding incident logs. The DSL and deputy/deputies monitor all information logged on CPOMS.

13. Links with other policies

This online safety policy is linked to our:

● Safeguarding and Child Protection policy

● Anti-Bullying policy

● Staff disciplinary procedures

● Data protection policy and privacy notices

● Complaints procedure

● E-Safety and Social Media Guidance

● Safer Working Practice in Schools Guidance 2019

● Data Storage and Retention Policy

● Staff Handbook

14. Use of digital and video images - Photographic, Video

The school is responsible for the safe use of photographic and video images of all pupils. When using photographic and video images staff must:

● follow school policies concerning the sharing, distribution and publication of those images. Images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.

● ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

● pupils must not take, use, share, publish or distribute images of others without their permission .

● must ensure pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

● ensure that written permission from parents or carers has been obtained before photographs of pupils are published.

15. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• Kept no longer than is necessary

• Processed in accordance with the data subject's rights

• Secure

• Only transferred to others with adequate protection.

• At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

• Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

• the data must be encrypted and password protected

• the device must be password protected

• the device must offer approved virus and checking software

• the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

16. Communications

When using communication technologies the school considers the following as good practice:

• The official school email service (Office 365) is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

• Users need to be aware that email communications may be monitored

• Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

• Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging (Unless school mobile) or public chat / social networking programmes must not be used for these communications.

• Only official email addresses should be used to identify members of staff.

17. Inappropriate Use

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

17.1 User Actions:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

● child sexual abuse images

● promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation

● adult material that potentially breaches the Obscene Publications Act in the UK

● criminally racist material in UK

● pornography

● promotion of any kind of discrimination

● promotion of racial or religious hatred

● threatening behaviour, including promotion of physical violence or mental harm

● any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

● Using school systems to run a private business

● Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school

● Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions

● Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)

● Creating or propagating computer viruses or other harmful files

● Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

● On-line gaming (educational)

● On-line gaming (non educational)

● On-line gambling

- Use of social networking sites (Unless for managing school pages)
- Use of video broadcasting e.g. YouTube unless agreed by senior management

18. Remote Learning

During periods of remote education, measures are in place and must be adhered to in order to safeguard pupils and teachers online.

This guide will be shared with parents and carers and studied by staff prior to the commencement of any online contact with pupils during periods of home learning

Appendix 1

Online Safety – Classroom Rules

When I use the school's ICT systems (like iPads and laptops) to access the internet in school

I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or another adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a laptop or iPad when I'm finished working on it
- Understand that I must be socially responsible with regard to using the internet, including treating others with respect, and reporting instances of online bullying.
- Understand that irresponsible use of the internet will result in the loss of Internet access.

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

- I will hand my mobile phone to my teacher at the start of the school day and not use this on school premises

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Use any inappropriate language when communicating online
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

Appendix 2

Online Safety

How to keep safe online – Things to consider…..

What could they find out?

If you post stuff online, think about how much people could find out about you from it.

Have you posted about your favourite music or sports? Remember, people do lie online and the more information they have about you the easier it is for them to trick you!

Don't say too much

If you're chatting to someone, don't tell them anything which could help them find you in the real world – things like your full name, school, email address or even photos.

Remember, even if you've been chatting for ages you still can't be sure that they aren't up to no good.

Be careful on camera

It can be unsafe to video chat with people you meet online. Some people will threaten to share a private video or picture with other people if you don't do what they say. If anyone threatens you in this way they are breaking the law and you should report them to CEOP. Whatever has happened, you won't be in trouble!

Don't meet up without an adult you trust.

People do lie online so it's always risky to meet up face to face with someone you've met online. If you do meet up with someone, make sure you do it in a busy public place and take an adult you trust with you. If you take a friend you could put them at risk as well. Tell the person you're meeting you want to meet in a public place and that you're brining an adult with you. Anyone who genuinely wants to be friends should understand that you want to make sure you are safe.

Block and report

Most websites you chat on will let you 'block' other people if you don't want to talk to them anymore. Learn how to do this on any sites and apps you use. If someone makes you feel uncomfortable or upset 'block' them and tell an adult.

Know how to report

No matter how long you've been chatting and whatever has happened it's never too late to seek help if someone starts being weird with you, makes you feel uncomfortable, worried or frightened. **If you don't want to talk to an adult at home, there are lots of adults in school that will help.** If you talk to the adults in your class or someone else you feel comfortable with, they will speak with Mr Hinchcliffe, who's main job in our school is to make sure that children feel happy and safe both at school, and at home!

You can always phone **Childline on 0800 1111** or report to **CEOP**. You won't be in trouble. Honest!

Appendix 3

Online Safety

8 steps to keep your child safe online

1. **Explore together**: Ask your child to show you their favourite websites and apps and what they do on them. Listen, show interest and encourage them to teach you the basics of the site or app.

2. **Chat little and often about online safety**: If you're introducing them to new learning websites and apps while school is closed, take the opportunity to talk to them about how to stay safe on these services and in general. Ask if anything ever worries them while they're online. Make sure they know that if they ever feel worried, they can get help by talking to you or another adult they trust.

3. **Help your child identify trusted adults who can help them if they are worried**: This includes you and other adults at home, as well as adults from wider family, school or other support services who they are able to contact at this time. Encourage them to draw a picture or write a list of their trusted adults.

4. **Be non-judgemental**: Explain that you would never blame them for anything that might happen online, and you will always give them calm, loving support.

5. **Supervise their online activity**: Keep the devices your child uses in communal areas of the house such as in the living room or kitchen where an adult is able to supervise. Children of this age should not access the internet unsupervised in private spaces, such as alone in a bedroom or bathroom.

6. **Talk about how their online actions affect others**: If your child is engaging with others online, remind them to consider how someone else might feel before they post or share something. If they are considering sharing a photo/video of somebody else, they should always ask permission first.

7. **Use 'SafeSearch'**: Most web search engines will have a 'SafeSearch' function, which will allow you to limit the content your child can access whilst online. Look out for the 'Settings' button on your web browser homepage, which is often shaped like a small cog.

8. **Parental controls**: Use the parental controls available on your home broadband and all internet enabled devices in your home. You can find out more about how to use parental controls by visiting your broadband provider's website.

If you need further support with online safety for your child, please speak with school staff and they will direct you to our **Parent Support Advisor – Lauren Dean** or our **Safeguarding Lead – Andy Hinchcliffe**