# Humberston C of E Primary School
# E-Safety Policy

Agreed by Governors June 2023
Last Review: January 2025
Next Review: June 2027

# The Humberston C of E Primary School

# E-safety Policy

## Contents


| | |
|---|---|
| **Introduction** | **3** |
| **Legislation and Guidance** | **4** |
| **Development, Monitoring and Review** | **4-5** |
| **Roles and Responsibilities** | **5-9** |
| **Curriculum** | **9** |
| **Educating pupils about online safety** | **9-10** |
| **Educating parents/carers about online safety** | **10-11** |
| **Cyber-bullying** | **11-13** |
| **AI (Artificial Intelligence)** | **13** |
| **Acceptable use of the internet in school** | **13-15** |
| **Monitoring arrangements** | **15** |
| **Links with other policies** | **15** |
| **Communications** | **16-17** |
| **Appendices** | **18-21** |

## Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The e-safety policy that follows explains how we intend to manage and reduce these risks, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use. It should be read in conjunction with the following documents and policies

- Computing policy.
- Acceptable Use Agreement.
- Anti-Bullying / Safeguarding Policy.

## 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 and school staff
- Relationships
- 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.

This policy also takes into account the National Curriculum computing programmes of study.

## Development, Monitoring and Review

This E-Safety policy has been developed by the following:

- School Computing Subject Leader (E-Safety Coordinator)
- Headteacher

It will be made available to the whole school community through the following:

- Staff meetings
- Governors meeting
- School website

## Schedule for Development, Monitoring and Review

| | |
|---|---|
| This E-Safety policy was approved by the Governing Body/Governors Sub Committee on: | Spring Term 2025 |
| The implementation of this E-Safety policy will be monitored by the: | ICT Subject Leader & E-safety Committee |
| Monitoring will take place at regular intervals: | Annually by the Strategic Lead – ICT in Schools |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | June 2026 |
| Should serious E-Safety incidents take place, the following external persons/agencies should be informed: | LA Safeguarding Officer<br>Local Police<br>Trust Safeguarding Lead |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Staff training

## Scope of the Policy

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

The Head teacher is empowered, to such extent as is reasonable, to regulate the behaviour of students/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 is 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.

## Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school.

### Governors:

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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 governing board 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 governing board will co-ordinate regular meetings with appropriate staff to discuss online safety requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must 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 service providers and IT staff 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 systems 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 governor who oversees online safety is **Claire Wong**.

The role of the E-Safety Governor will include:

- regular contact with the E-Safety Co-ordinator regarding E-Safety incidents
- reporting to relevant Governors committee

All governors will:

- Ensure that 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.

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or 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.

**Headteacher:**

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the whole school. It is also the headteachers role to:

- Takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies/documents;

- Leads the E-Safety committee;

- Liaises with the Local Authority;

- Communicates regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs;

- Attends relevant meeting/committee of Governors;

- Regularly monitor the use of the network, internet and emails in order that any misuse/attempted misuse can be reported for investigation and possible sanction.

**E-Safety Coordinator**:

- Must ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place;

- Provides training and advice for staff;

- Promote E-Safety to all pupils within the school and how to stay safe online.

**The ICT manager:**

The ICT 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 monthly 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.

**All staff and volunteers:**

All staff, including contractors and agency staff, and volunteers are responsible for ensuring that:

- 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 terms on acceptable use.

- 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 and processes failing by reporting the incident on CPOMS for the DSL to be made aware.

- Following the correct procedures by asking permission from the headteacher if they need to bypass the filtering and monitoring systems for educational purposes.

- 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.

- 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.

**The designated safeguarding lead (DSL) –**

Details of the school's designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

- Working with the ICT manager to make sure the appropriate systems and processes are in place

- Working with the ICT manager 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 policy

- 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 and delivering staff training on online safety

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

- Providing regular reports on online safety in school to the governing 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.

**Pupils:**

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

**Parents/Carers:**

Parents/carers 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 terms on acceptable use of the school's ICT systems and internet

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
- Parent resource sheet – Childnet

**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.

## Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should inform the Headteacher and e-safety co-ordinator.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## Educating pupils about online safety

**Pupils**

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

In Key Stage (KS) 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 (KS) 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or Google Classrooms. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- 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/carers 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.

## 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 also the school behaviour policy.)

### 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/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

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

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, 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 headteacher
- 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 headteacher 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 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 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.

**AI (Artificial intelligence):**

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.

Humberston CofE Primary School 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.

Humberston CofE Primary School will treat any use of AI to bully pupils in line with our behaviour 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 the school/trust.

## Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's 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 and restrict access through filtering systems where appropriate.

**Pupils using mobile devices in school**

Mobile devices are not permitted within the school unless the pupil is in Year 6. They will be required to give their device to their teacher who will firstly ensure that the phone is on silent, then put it in a box in a cupboard. The device will be given back to the pupil at the end of the school day.

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.

**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)

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

- Not sharing the device among family or friends
- Make the device available as requested for the IT Manager to install anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

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 the ICT manager.

**How the school responds 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 and computing policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's 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 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**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:

1. Abusive, threatening, harassing and misogynistic messages
2. Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
3. 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 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 child protection and safeguarding policy.

**Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety via CPOMS.

This policy will be reviewed every year by the Computing Lead. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

**Links with other policies**

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Computing and internet acceptable use policy

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

| | Staff & other adults | | | | Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| **Communication Technologies** | Allowed | Allowed in social time | Allowed for professional/ educational purposes | Not allowed | Allowed | Allowed for educational purposes with staff permission | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | X | | | | | | X | |
| Use of mobile phones in school | | X | | | | | | X |
| Use of mobile phones for personal use | | X | | | | | | X |
| Taking photos on other camera devices | | | X | | | X | | |
| Use of hand held devices eg PDAs, PSPs | | | X | | | X | | |
| Use of personal email addresses in school, or on school network | X | | | | | | X | |
| Use of school email for personal emails | | | | X | | | X | |
| Use of chat rooms/facilities | | | X | | | X | | |
| Use of instant messaging | | | X | | | X | | |
| Use of social networking sites | | | X | | | X | | |
| Use of blogs | | | X | | | X | | |
| Use of chat rooms, instant messaging, social networking sites or blogs for personal use | | X | | | | | | X |

| **Unsuitable/Inappropriate Activities**<br><br>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:<br><br>User Actions | | Acceptable | Acceptable at certain times | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| 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 | | | | X |
| | promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse & fraud legislation | | | | X |
| | adult material that potentially breaches the UK Obscene Publications Act | | | | X |
| | criminally racist material in UK | | | | X |
| | pornography | | | X | |
| | promotion of any kind of discrimination | | | X | |
| | promotion of racial or religious hatred | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | X | |
| | 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 | | | X | |
| Using school systems to run a private business | | | | X | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | X | |
| Carrying out sustained or instantaneous high volume network traffic (downloading /uploading files) that causes network congestion & hinders others in their use of the internet | | | | X | |
| On-line gaming (educational and non-educational) | | | X | | |
| On-line gambling | | | | X | |
| On-line shopping | | | X | | |
| File sharing | | | X | | |
| Use of social networking sites | | | X | | |
| Use of video broadcasting e.g. Youtube | | | X | | |

Appendix 1:

## E-LEARNING CODE OF CONDUCT AGREEMENT

**NAME OF PUPIL:** _____

**Parent:**

As parent or guardian, I have read, discussed and explained the Acceptable Use Agreement to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access may be withdrawn and I will be informed.
I understand that systems are in place to prevent pupils from accessing inappropriate materials but that it is not possible to provide a 100% assurance as pupils may accidentally come across material which would be inappropriate. In such instances staff will follow school procedures to prevent this happening in the future.

Parent/Guardian Signature _____ Date _____

**Permission and Copyright Release**
I consent to photographs and digital images of my child named above, appearing in printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as CD-ROM, as part of the promotional activities of the school.
I also consent to examples of my child's work being published on the school website or in other media, subject to strict confidentiality of personal information.

Parent/Guardian Signature _____Date _____

**<u>Digital Use by Parents</u>**

**Taking of Digital Recordings**
I accept and agree to my child being captured in school performance recordings filmed by other parents, I understand that whilst filming their own children my child's image may be included in that recording.

Parent/Guardian Signature_____ Date_____

**Use of Digital Recordings**
I agree that any digital video filmed by myself during school performances will be used solely for home use and not under any circumstances published to any exterior media.

Parent/Guardian Signature_____ Date_____

**Digital Video**
I consent to my child taking part in Humberston CE Primary School projects using digital video. I consent to my child taking part in and appearing in the production of digital videos. I understand that video may be made available on the school website or used in other school promotional activities.

Parent/Guardian Signature _____Date _____

## ACCEPTABLE USE AGREEMENT – PUPILS

**I WILL**



Always follow the instructions of my teacher



Always be nice and polite when I send messages to other users.



Always tell my teacher if I see, hear or read anything which makes me feel uncomfortable while using technology.



Always check with my teacher before using websites.



Close laptops and iPads down properly or log out when I have finished using them.



Remember that the information I read on the internet may not always be right.



Check with an adult before

* sending e-mail
* downloading files
* completing questionnaires or subscription forms
* opening e-mail attachments
* printing anything out

**I WILL NOT**



Send any member of the school a message which is not nice. I understand that this includes messages sent from home.



Use bad language in a message.



Use any other person's work or e-mail.



Tell a stranger any of the following information:

- my name, home address or telephone numbers
- any other personal information about myself or any of my friends.

**REMEMBER – YOUR TEACHERS CAN SEE AND MONITOR YOUR WORK AND INTERNET USE**

Name of pupil ……..

Signature:

……..……..Date:……

Appendix 2:

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS | |
|---|---|
| **Name of staff member/governor/volunteer/visitor:** | |
| **When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**<br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)<br>• Use them in any way that could harm the school's reputation<br>• Access social networking sites or chat rooms<br>• Use any improper language when communicating online, including in emails or other messaging services<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network<br>• Share my password with others or log in to the school's network using someone else's details<br>• Take photographs of pupils without checking with teachers first<br>• Share confidential information about the school, its pupils or staff, or other members of the community<br>• Access, modify or share data I'm not authorised to access, modify or share<br>• Promote private businesses, unless that business is directly related to the school | |
| 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.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>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.<br>I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>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/governor/volunteer/visitor):** | **Date:** |

Appendix 3:

| 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, governors 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? | |