Hoyland Springwood Primary School
e-Safety Policy

Hoyland Springwood Primary School is committed to safeguarding all members of the school community. The Internet and other digital and information technologies are greatly beneficial tools to children's learning but children need to be aware of how to use these tools appropriately and safely. This e-safety policy highlights how Hoyland Springwood Primary School educates children, parents and staff about the benefits, risks and responsibilities of using information technology. Mrs Jennifer Hunt is the designated eSafety Co-ordinator.

Teaching and Learning

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Information will be provided to parents about how to educate and support their children with safe internet use.

eSafety and Safeguarding messages in learning activities are embedded across all areas of the curriculum, including making sure that all pupils will understand the dangers of radicalisation and exposure to extremist views; learning about key British Values to build resilience against these views and knowing what to do if they experience them (in line with Prevent).
To keep up to day with the most recent KCSIE, making sure current issues (such as County Lines and Peer-on-Peer abuse) are monitored and addressed through eSafey lessons.
We will provide a series of specific eSafety-related lessons in every year group as part of the PSHE curriculum, as well as e-Safeguarding specific lessons when necessary within a specific class in order to address any issues that have arisen. Where appropriate, messages around eSafety will children will also be focussed on current issues from the most recent KCSIE document (eg PREVENT, County Lines and Peer-on-Peer abuse).

How can Internet use enhance learning?

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Hoyland Springwood Primary School Website and Facebook

The school has sought parental consent for any images of children that are used on the school website and Facebook. To ensure the children's safety no full names will be published on either site.

How will pupils learn how to evaluate Internet content?

Pupils will be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Pupils should compare web material with other sources and be able to evaluate which is more useful. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas.

All pupils will be taught that if they access any information or images which they think are inappropriate or make them uncomfortable, they should close the page and report the incident immediately to the teacher who will pass the report onto the e-safety coordinator and the headteacher.

How will e-mail be managed?

Email is an essential means of communication for both staff and pupils. Whole-class or group e- mail addresses will be used at Hoyland Springwood Primary School. Pupils will be taught in school how to safely use e-mail at home and guidance will be provided to parents.

How will social networking and personal publishing be managed?

The school will block/filter access to social networking sites. However, parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Pupils will be taught about personal safety when using social networking sites outside the school and offer appropriate advice

Pupils will learn:

- never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- never to communicate or meet people they do not know.
- not to place personal photos on any public social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- about security and be encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

How will filtering be managed?

The school uses Lightspeed filtering to ensure inappropriate material is denied to pupils and Bull TCL monitor and block any inappropriate sites.

If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator who will contact Bull to block the site.

How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How will Internet access be authorised?
Within the Foundation Stage, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resultingfrom Internet use.

The school carries out regular audits to ensure that the eSafety policy is adequate and that it is implemented appropriately.

How is the Internet used?

The school will liaise with local organisations to establish a common approach to e-safety.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

- Pupils will only use the internet sites provided by staff which have been checked; this will include search engine sites.
- All pupils will follow the e- safety rules.

How will the policy be introduced to pupils?
All pupils will be taught about e-safety regularly and will help to design posters about safety rules. The school's eSafety curriculum makes use of a wide range of engaging resources in order to engage children. The school will follow closely the advice given by The Child Exploitation and Online Protection Centre relating to online safeguarding. These sites will also be promoted to parents and information regarding e-safety in the home will be shared.

- e-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme is in place to raise the awareness and importance of safe and responsible Internet use.
- Instruction in responsible and safe use should precede Internet access.

How will the policy be discussed with staff and governors?
The e-Safety Policy and its application and importance will be discussed with staff and governors. All staff will continue to receive training, either online or face to face, in relation to e-Safety. eSafety training is made available to governors. The school has a named Safeguarding Governor whose responsibilities include eSafety. This is currently Mrs Michelle Jones.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school prospectus and on the school website/blogs.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- Support for parents will be provided as and when needed.
- A partnership approach with parents will be encouraged and guidance on Internet use in the home will be issued.

eBehaviour Agreements

In order to ensure that pupils, parents, staff and volunteers clearly understand their responsibilities in relation to eSafety, eBehaviour Agreements and used and signed regularly (usually every 2 years and annually for staff).

The eBehaviour agreements are in different forms and feature as appendices in this policy:

- eBehaviour for pupils
- eBehaviour for parents
- Acceptable use for staff and volunteers
- Zoom acceptable use policy for staff
- Zoom acceptable use policy for pupils and parents
- Seesaw acceptable use for all

Date approved by the Governing Body: _____

This policy is to be reviewed Summer Term 2023

Signed:

Chair of Governors: _____

Head teacher: _____

Hoyland Springwood Primary School - Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (a strong password has numbers, letters and symbols, with 8 or more characters and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware, without permission from the system manager or Headteacher.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace or accessed remotely. Any data which is being removed from the school site (such as via email) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information on any personal devices (such as laptops, digital cameras). I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.
- I will adhere to the eSafety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead, Mrs Jennifer Hunt, as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and Trust ICT Technician, Mr Michael Haworth, who is responsible for filtering, as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the Headteacher as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Headteacher.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, the Trust or the Local Authority, into disrepute.).
- I will promote eSafety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practice online, either in school or off site, then I will raise them with the Headteacher.
- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the Trust's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Hoyland Springwood Primary School - eBehaviour Agreement for Volunteers

I understand that I must use the school ICT systems and resources in a responsible way in order to ensure the safety of pupils, staff, volunteers and the ICT systems.

Access to ICT Equipment & Resources

- I will only use school ICT systems and equipment for purposes directly linked to my volunteer role. I will not use school resources for personal use.
- I will use ICT resources as directed by school staff and for the intended purpose(s) only.
- I will report any breakages or faults with ICT equipment to a member of the office staff immediately.
- I will not access, or attempt to access, any files or aspects of the computer system which are not directly linked to my volunteer role.

Safeguarding Others

- I will not disclose any confidential or personal information relating to others or the school.
- I will not upload or download any material without the express permission of a member of the Senior Leadership Team.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings unless I have the express permission of a member of the Senior Leadership Team.

Supporting Children in their Use of ICT

- I will support and encourage children to use ICT systems and equipment sensibly and in line with school policy.
- I am aware of the eBehaviour agreements for pupils and will ensure that any children with whom I am working follow this.

Personal Online Safety

- I understand that my use of the ICT systems, internet and e-mail may be monitored.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report to a member of the Senior Leadership Team any unpleasant or inappropriate material or messages or anything that I find offensive.
- I will not use my mobile phone in school when I am working with students

I understand that if I fail to comply with this Acceptable Use Policy Agreement, my voluntary placement may be withdrawn and access to school systems suspended. I have also read, understood and agree to comply with the Barnsley Safeguarding Board guidance relating to use of Social Networking sites.

Hoyland Springwood Primary School

eBehaviour Agreement for Foundation Stage & Key Stage 1 Pupils

I must use computers, mobile phones and technology responsibly, to help me and others stay safe.

- I will be kind and polite to other people when I am using the internet on computers, iPads or other devices.
- I will tell an adult if I see anything that worries me, or if anyone is unkind to me.
- I will listen to my teacher or other adults and follow instructions when using the computers and iPads in school.
- I will not talk to strangers on the internet.
- I will not tell other people on the internet information such as my full name, date of birth, or address.
- I will only use the programmes and visit the websites that my teacher or another grown up has said I can use.

How does school help me to stay safe?

- Teachers and other adults in school will help me if I am upset by something I see on the computer or if someone is unkind to me.
- School will provide a safe computer system for me to use.
- School will take speak to me and my parents if I break the rules or am unkind to other children.

Hoyland Springwood Primary School

eBehaviour Agreement for KS2 Pupils

I must use computers, mobile phones and technology responsibly, to help me and others stay safe.

- I will treat my password like my toothbrush – I will not share it or try to use anyone else's password.
- I will be polite and responsible when I communicate with others.
- I will tell an adult if I see anything I am unsure about including:
  - damage to equipment
  - upsetting images or text
  - websites that are not allowed
- I will report bullying whether it is to me or others including:
  - online bullying
  - email bullying
  - text bullying
- I will listen to the responsible adult and follow instructions when using a PC or other technology.
- I will not talk to strangers online.
- I will not share any personal information such as my full name, date of birth, or address.
- I will not agree to meet with anyone in person I have met online unless I have agreed this with and am accompanied by a parent/carer.
- I will not use school equipment for personal use unless I have permission from a responsible adult, including: games, file sharing, video broadcasting, social networking e.g. Snapchat, Facebook, chat or instant messenger etc…
- I will not upload or download files that may be upsetting to others.
- I will not open attachments unless I know who sent them.
- I will not bully other people, verbally, physically or with technology such as the Internet, email or mobile phones.
- I will not send or forward unpleasant/inappropriate texts or photos to other people.

How does school help me to stay safe?

- **Teachers and other adults in school will provide support to me or anyone else, if I am upset by images, text or am a victim of bullying.**
- **School will provide a safe network and monitor my use of computers, iPads and the internet.**
- **School will take action against me or others if I use the Internet or mobile phone to bully, or break any of the rules above.**

Signed _____

Name: _____

Date: _____