HAYFIELD LANE PRIMARY

E-Safety Policy

Date of issue: January 2023	Review: January 2024

E-SAFETY

We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. (Teaching Online Safety in Schools DFE: Jan 2023)

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. To do this, pupils and staff must be educated for critical and responsible ICT use wherever the user of the technology may be.

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children may include:

- The Internet
- Mobile phones
- Digital cameras
- E-mail
- Instant messaging
- Web cams
- Blogs
- Podcasting
- Social networking sites
- Video broadcasting sites
- Cloud based storage system
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Ipads and other tablet devices
- Ipods that are "internet ready"
- Smart phones with e-mail, web functionality and cut down 'Office' applications

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- The direct teaching of e-Safety for pupils.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinators at Hayfield Lane Primary are Mrs Tempest (Head) and Mrs John Lewis (Deputy Head).

This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: curriculum, child protection, behaviour, health and safety and anti-bullying.

All teachers are responsible for promoting, teaching and supporting safe behaviours in their classrooms and following school e-Safety procedures. All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking;
- Safe use of school network, equipment and data;
- Social media policy
- Acceptable usage agreement
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- Bullying / Cyberbullying procedures;
- Their role in safeguarding pupils
- Their role in providing e-Safety education for pupils.
- Staff Code of Conduct
- Parent Code of Conduct

Staff are reminded / updated about e-Safety matters annually as part of safeguarding training and as part of the induction process for new staff.

The school provides opportunities within the curriculum to teach about e-safety. This included regular Tribe Time (class assembly) sessions where the Project Evolve resources for each year group are used. The teaching of e-safety is always age and developmentally appropriate.

Managing the Internet Safely - The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. An environment where misinformation and disinformation can flourish. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people. Much of the material on the Internet is published for an adult audience and some is

unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

Technical and Infrastructure:

This school:

- Maintains filtered broadband connectivity managed through ACS;
- Ensures their network is 'healthy' by having health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator (ACS) checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device; - Never allow children to use internet facilities without supervision.

Policy and Procedures:

Hayfield Lane Primary School:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff previews sites whenever possible before use [where not previously viewed and cached]
- Plans the curriculum context for Internet use to match pupils' ability, using child friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering
- Ensures the named child protection officer has appropriate training;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities.

Education and training:

This school:

- Fosters an environment that encourages pupils to tell a teacher / responsible adult. immediately if they encounter any material that makes them feel uncomfortable.
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or other school adult.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident.
- Ensures children are aware of what online and cyber bullying are and how to report abuse.
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on national guidance.
- Has a culture and ethos that is about partnering with families and the local community to ensure that e-safety messages include all aspects of school life.

Pupils are taught a range of skills and behaviours appropriate to their age and experience based on the key guidance from *Teaching Online Safety in Schools (DFE: Jan 2023),* such as:

- How pupils evaluate what they see online. For example, pupils will explore the reasons for something being posted, whether a person is who they say they are and how to identify if something that they have seen is fact or opinion.
- How to recognise techniques for persuasion. For example, techniques used by companies to persuade people to purchase items, ways to protect themselves from online criminal activities as well as understanding what misinformation and disinformation is.
- Understanding what acceptable and unacceptable behaviour online looks like. For example, that the same standards of honest and respect apply on and offline. To recognise unacceptable behaviour in others.
- How to identify online risks. For example, how their behaviour online could put them at risk or a have an impact on their digital footprint. Alternatively, how the behaviour of another online user could put them at risk such as cyber criminals.
- How and when to seek support. For example, pupils being able to identify who trusted adults are so that they can seek support from them if they are concerned or upset by something that they have seen online.
- How to develop online media literacy strategies and to understand what is meant by personal data. For example, understanding the risks of sharing personal information and strategies that can be used to protect their privacy. Alongside that, understanding how to participate safely and positively within online environments.
- Understanding how personal data can be used. For example, recognising how personal data is collected as well as how and why it is sold by different companies.
- How to navigate the internet and manage information. For example, understand why age verification exists as well as what is meant by copyright and ownership.
- How content can be used and shared. For example, how a digital footprint can have an impact on future prospects as well as how difficult it is to remove something that has been posted. The importance of having a positive online profile.
- The importance of password protection. For example, why passwords are necessary and how to ensure that they are as secure as possible. Also, understanding

how other online users may use strategies to get someone to reveal their password and the harm that can be done from this.

- How app and online games are designed to keep users online. For example, discussing the monetary value of keeping players online for as long as possible as well as how designers use updates and notifications to draw users back to platforms.
- Understanding the importance of privacy settings. For example, exploring the limitations of privacy settings and where to find privacy settings for different sites.
- How to deal with online abuse. For example, how to respond to online abuse even when it is anonymous and being clear about what good and bad online behaviour looks like.
- Understanding that not everyone is who they say they are online. For example, exploring why fake profiles are created and how to look out for them.
- Recognising what is meant by unsafe communication. For example, having safe strategies for staying safe online when communicating with other people, especially those that they do not know or have never met. Alongside understanding why sharing your address, phone number and email address is a risk as well as being able to explain that communicating safely online and protecting
- Recognising the impact that online content can have on your wellbeing. For example, recognising how image filters and digital enhancements are used to create 'unrealistic' online images.
- Understanding the impact that spending too much time online can have. For example, the children evaluating how much screen time they have access to as well as considering how this affects mental health and relationships.
- Understanding how search engines work. For example, to know some search engines / web sites that are more likely to bring effective results and to know how to narrow down or refine a search.
- Knowing not to download any files without permission. For example, audio or video files.

Security, Data and Confidentiality:

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018

-

Copyright and Plagiarism

This school:

- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
  ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; on- line gaming / gambling;
- runs a rolling programme of advice, guidance and training for parents, including:
- information in school newsletters; on the school web site;
- demonstrations, practical sessions held at school;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

Managing e-mail

The use of email within school is an essential means of communication for staff.

Pupils currently only have access to Purple Mash email accounts when it arises within the curriculum and all communication is monitored by staff during these lessons

Staff must use the school's approved and secure email system for any school business.

Staff must inform (the e-safety co-ordinator/ line manager/ ICT Manager) if they receive an offensive or inappropriate e-mail.

If any threatening emails (terror related) are received by the school, the Emergency Plan will be followed, ensuring the LA are informed alongside the Police via 101.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. We strongly recommend, as a school, that parents look at age related guidelines for social media apps and use them as a guide to whether they are acceptable for their children before they approve app requests. Those guidelines are there to safeguard young children due to the negative impact these platforms can have on the mental health of young people.
Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves

-

the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Use of Digital and Video images

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- The school web site complies with the school's statutory requirements
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities are not published;
- Photographs published on the web do not have full names attached;
  We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored on the network and may kept for a school publications;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website or MLE;
- We do not include the full names of pupils in the credits of any published school produced videos

Creation of videos and photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes school trips. School's own mobile devices must be used in this case.

Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

-

Pupils' names will not be published alongside their image and vice versa on the school website, twitter account, mobile app or any other school-based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops.

Managing equipment

Our internet access is provided by ACS.

ACS manage the administrative devices throughout school and also curriculum access.

Our ICT Support provider (ACS) follows DfE advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, e-safety co-ordinator or the ICT Manager. *The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.*

To ensure the network is used safely this school:

- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that pupils should never be allowed to log-on using teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off or lock a computer when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then logon again as themselves.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and that they inform the ICT technician otherwise;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is only sent within the approved secure system in our LA;
- Reviews the school ICT systems and policies regularly with regard to security.

-

Handling of Infringements

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. These will be in line with other related policies such as the acceptable use agreement.

Pupil's possible infringements:

- Use of non-educational or personal sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it
- Deliberately corrupting, removing or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

All infringements will be dealt with following the school behaviour policy; infringements of a more serious nature will be dealt with by a member of SLT and reported to the DSP if appropriate.

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site

2. Inform DSL as appropriate

Other safeguarding actions:

1. Secure and preserve any evidence

2. Inform the sender's e-mail service provider

Staff Level 1 infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal social media sites, house moving sites, personal email, instant messaging etc.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community.

-

- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection

Sanction - **Referred to Headteacher / Governors and follow school disciplinary procedures;**

Discuss with HR advisor, report to Police.

Possible safeguarding actions:

- Remove the source to a secure place to ensure that there is no further access to the PC, laptop or tablet.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they may be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Human Resources Advisor.

Child Pornography

In the case of Child Pornography being found, the member of staff should be **immediately suspended,** and the Police should be called:

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP) and to the LADO.

-

How will staff and pupils be informed of these procedures?

They are fully explained and included within the school's e-safety / Acceptable Use Policy.

- All staff will be required to sign the school's e-safety Policy acceptance form.
- Pupils are taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'.
- Pupils will sign an age appropriate e-safety / acceptable use form.
- The school's e-safety policy is made available on the school website, and parents will sign an acceptance form when their child starts at the school, to allow access to the internet
- Information on reporting abuse / bullying etc. is made available by the school for pupils, staff and parents.

Assessing risks

The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse are dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents are informed of the complaints procedure, which is available on the school website

Curriculum

E-safety is built into existing lessons throughout the curriculum, but it is also covered within specific online safety sessions as well as being covered through school-wide approaches. Each academic year pupils further online knowledge using the 'Project Evolve – Education for a Connected World' framework. The framework aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience and effects positive culture change. The objectives promote the development of safe and appropriate long-term behaviours, and support educators in shaping the culture within their setting and beyond.

Within each year group topics include:

- **Self-Image and Identity** - This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media

-

influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

- **Online Relationships** - This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
- **Online Reputation** - This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.
- **Online Bullying** - This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.
- **Managing Online information** - This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.
- **Health Well-being and Lifestyle** - This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.
- **Privacy and Security** - This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.
- **Copyright and Ownership** - This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

Children's understanding of E-Safety will be assessed through pupil voice conversations as well as year group specific assessment criteria by the class teacher.

Inclusion

All pupils will have access to E-Safety regardless of gender, race, cultural background or any physical or sensory disability. The curriculum and activities provided will be differentiated, in accordance to the needs and abilities of each pupil through: task, outcome, pupil groupings, additional support and equipment.

Leadership

The Leadership Team will:

- Support staff in the delivery of the E-safety curriculum

-

- Provide Inset and training as required through CPD and drop in sessions
- Monitor the provision of E-Safety throughout the school, by looking at planning, PSHE books and talking to pupils
- Monitor the use of resources and provide new resources as appropriate
- Liaise with the ICT technician to monitor the security level used in school to ensure the safety of our learners.

The Learning Community

All staff have copies and access to the school e-safety policy and know its importance. Staff are aware that internet traffic can be monitored and traced to individual users. Parents' attention is drawn to the school e-safety policy in newsletters, and on the school website. The school liaise with local organisations to establish a common approach to e-safety.