Haydn Primary School
Digital Safety Policy

1. 1 Writing, monitoring and reviewing the digital safety policy

1.1.1 Development of the policy

This digital safety policy is part of the School Development Plan and relates to other policies including those for ICT, Safeguarding, Anti-Bullying, Curriculum and Data protection and security

- This digital safety policy has been written on behalf of the school by the Computing co-ordinator, who is also the designated digital safety Co-ordinator; in consultation with the Headteacher, Safeguarding Officer, Staff (including teachers, support staff and technical staff), Governors, parents/ carers and pupils.
- It was approved by the Governors on ...

1.1.2 Reviewing the policy

- The policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of new technologies, new threats to digital safety or incidents that have taken place.
- The next review date is July 2022.

1.1.3 Monitoring the impact of the policy

- A log will be maintained to record reported incidents.
- Serious incidents will be referred to the appropriate authorities.

1. 2 Scope of the Policy

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

1. 3 Roles and Responsibilities

1.3.1 Governors

- Governors are responsible for the approval of the digital safety policy and for reviewing its effectiveness.

1.3.2 Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including digital safety) of the members of the school community.
- The day to day responsibility for digital safety will be delegated to the digital safety co-ordinator
- The Headteacher and (at least) one other member of the senior leadership team should be aware of the procedures to be followed in the event of a serious digital safety allegation being made against a member of staff.

1.3.3 Digital Safety Co-ordinator

- Takes day to day responsibility for digital safety issues in liaison with the Safeguarding Officer and has a leading role in establishing and reviewing the school digital safety policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an digital safety incident taking place.
- Provides training and advice for staff.
- Liaises with the ICT technician
- Receives reports of digital safety incidents and creates a log of incidents to inform future digital safety developments
- Reports regularly to the Headteacher.

1.3.4 The IT Provider (presently NCC Schools IT)

Is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required digital safety technical requirements and any Local Authority Digital Safety Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering service applied is appropriate, effective and reasonable and is updated on a regular basis
- that they keep up to date with digital safety technical information in order to effectively carry out their digital safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is monitored in order that any misuse / attempted misuse can be identified.

1.3.5 Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of digital safety matters and of the current school digital safety policy and practices

- they have read, understood and signed the Staff Acceptable Use Agreement (AUP)
- they report any digital safety issues via the digital safety log or in the case of serious incidents to the Headteacher for investigation
- all digital communications with pupils and parents/ carers should be on a professional level and only carried out using official school systems
- digital safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the digital safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is logged so that filtering can be updated

1.3.6 Safeguarding Officer

- Is trained in digital safety issues and aware of the potential for serious child protection / safeguarding issues that can arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers potential or actual incidents of grooming
    - radicalisation
    - cyber-bullying
- Is responsible for disseminating WRAP3 training to all staff as part of the schools PREVENT duty and ensure that staff are aware of the ways in which pupils are vulnerable to radicalisation through social media (please see the safeguarding policy for further details)

1.3.7 Pupils

- are responsible for using the school digital technology systems in accordance with the school acceptable use rules and digital safety guidance
- should 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
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good digital safety practice when using digital technologies out of school and realise that the school's digital safety policy covers their actions out of school, if related to their membership of the school

- use of mobile phones on school premises is strictly prohibited. Any phones that are required to be brought to school must be stored in the school office during the school day. Year 6 are permitted to bring phones into school which must be locked in the phone safe during the school day.
- smart watches are not permitted on school premises. Children may use a fitbit or similar device that is a fitness tracker but does not have capabilities to connect to the internet or take any form of photo.

1.3.8 Parents/ Carers

- Parents /carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through training events, newsletters, letters, website and literature. Parents /carers will be encouraged to support the school in promoting good digital safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events

2. EDUCATION ,TRAINING AND COMMUNICATING OF DIGITAL SAFETY MESSAGES

2. 1 Pupils

2.1.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school recognises it has a duty to provide pupils with high-quality internet access as part of their learning experience in school and prepare them to make safe and effective use out of school.
- Internet use is part of the statutory curriculum and a necessary tool for staff and student.

2.1.2 Digital safety

The school recognises that whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in digital safety is therefore an essential part of the school's digital safety provision. Children and young people need the help and support of the school to recognise and avoid digital safety risks and build their resilience.

Digital safety should be a focus in all areas of the curriculum and staff should reinforce digital safety messages across the curriculum. The digital safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned digital safety curriculum will be provided as part of Computing / PHSE / other lessons and will be regularly revisited
- Key digital safety messages should be reinforced as part of a planned programme of assemblies and other class and whole school activities
- Digital safety rules and details of how to respond to concerns will be posted in all rooms where computers are used.
- Pupils should be taught in all lessons to be critically aware of the 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
- Pupils should be encouraged to adopt safe and responsible use both within and outside school
- Pupils will be taught how to keep themselves safe online both in and out of school and how to respond to concerns regarding unpleasant content or inappropriate contact.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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, 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Technician can temporarily remove those sites from the filtered list for the period of study.

2.2 Parents/ carers and the wider community

- The school recognises the essential role parents/ carers play in the monitoring and regulation of children's on-line behaviours out of school and that they may underestimate the dangers. The school will therefore seek to provide information and awareness to parents through information evenings, letters/ newsletters/ web site, curriculum activities, providing literature and drawing their attention to high profile events and campaigns.
- These events and resources will also be made available as appropriate to the wider community.

2.3 Staff/ Volunteers

- A planned programme of formal digital safety training will be made available to staff. This will be regularly updated and reinforced.
- An audit of the digital safety training needs of all staff will be carried out regularly.

- All new staff should receive digital safety training as part of their induction programme, ensuring that they fully understand the school's digital safety policy and Acceptable Use Agreements.
- The digital safety co-ordinator will receive regular updates through attendance at external training events and reviewing guidance documents released by relevant organisations.
- The digital safety co-ordinator will provide advice, guidance or training to individuals as required.

2.4 Governors

- Governors should take part in digital safety training or awareness sessions (in particular those governors responsible for technology, digital safety or safeguarding.

3.1 Technical – infrastructure/ equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the ICT technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at regular intervals. Pupils at KS1 and below will have a class logon.
- The administrator passwords for the school ICT system is kept by the IT Provider.
- The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users
- An appropriate system is in place for users to report any actual / potential technical incident / security breach.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- 'Guests' (for example, visitors and supply teachers are not allowed access to secure parts of the network and can only access using class logins. Trainee teachers undergoing a placement of 6 weeks or more are given a log-in to access the network, but not be given access to SIMs. This access is removed once the placement is finished.

- Only the IT Provider is able to install programmes on school devices.

3.1.1 Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

4 Publishing Content

4.1 Use of Digital and Video Images and Pupils' work

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully, using group photographs rather than photographs of individual children, and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

4.2 Published Content and the School Website

- The contact details on the school website should be the school address, email and telephone number. Staff or pupils personal information must not be published.
- The head teachers will take overall editorial responsibility and ensure that content is accurate and appropriate.

5 Communications

5.1 Email

- Email should be sent using the approved Schools IT service which is regarded as safe and secure and is monitored.
- Users must immediately report, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- If required as part of a learning activity, whole class email addresses may be used at KS1, while pupils at KS2 and above may be provided with individual school email addresses for educational use.
- Pupils should be taught about the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

5.2 Blogging

- Pupils will be explicitly taught about responsible and courteous behaviour while blogging and commenting on blogs and will sign an agreement before being allowed to use an approved blog.
- They will be warned that once they have posted a blog or comment they will not be able to remove it, and there will be consequences for inappropriate blogging or commenting.
- Staff will monitor blogs and comments posted and deal with any incidents of inappropriate posting.

5.3 Social Networking

5.3.1 Protection of Pupils

- Whilst pupils will not be allowed access to social networking sites in school, it is very possible that they will have access from home. As part of their digital safety curriculum they will be taught about the potential dangers posed by such sites and opportunities to communicate with strangers. This will include:
    - never to give out personal details of any kind which may identify them, their friends or their location
    - not to place personal photos on any social network space without considering how the photo could be used now or in the future
    - to only invite known friends and deny access to others when using social networking and instant messaging services
- Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications
- Pupils will be taught about how to respond to any inappropriate contact.

5.3.2 Use by Staff

- As part of their digital safety training staff will receive guidance on acceptable use, social media risks, checking of privacy settings, data protection and reporting issues.
- School staff should ensure that no reference is made in social media to pupils, parents/ carers or school staff.
- Staff should ensure that they do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions expressed by staff on social media should not be attributed to the school or local authority.
- Security settings on personal social media profiles should be regularly checked to minimise the risk of loss of personal information.

6 Data Protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (see Data Protection Policy for more information).

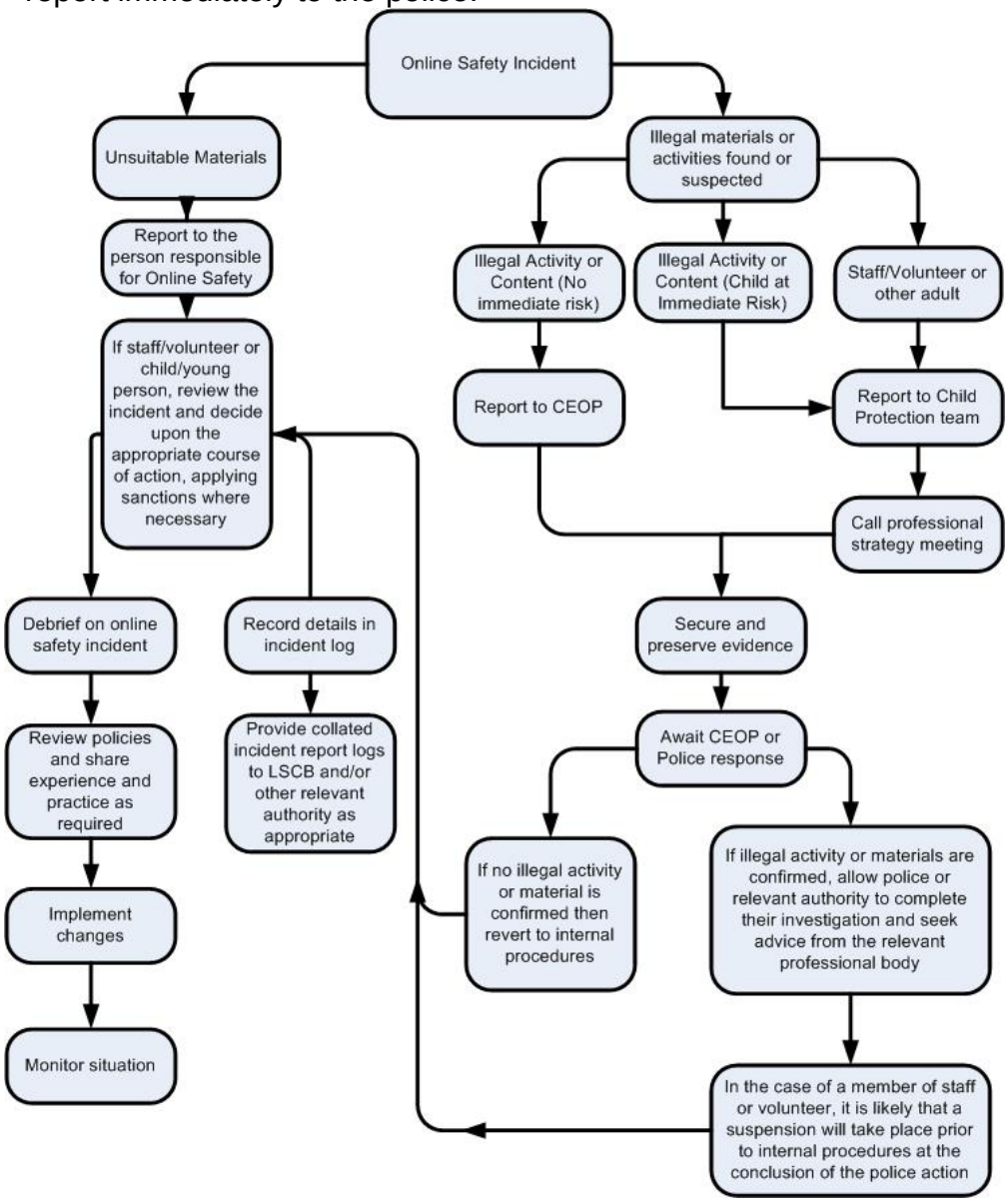
Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data (eg on memory sticks) using encryption and secure password protected devices.

7 Responding to incidents of misuse

7.1 Illegal Incidents

- If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



7.2 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

7.3 School Actions & Sanctions

- Most incidents are likely to involve inappropriate rather than illegal misuse. It is important that any incidents are logged and dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.
- It is intended that incidents of misuse involving pupils will be dealt with through normal behaviour / disciplinary procedures

This policy will be reviewed by the ICT co-ordinator and leadership team and shared with all stakeholders.

Signed:

Date: