COLESHILL HEATH SCHOOL
EVERY CHILD, EVERY DAY

ICT and ONLINE SAFETY POLICY

June 2022

Coleshill Heath School
Lime Grove
Chelmsley Wood
Birmingham
B37 7PY

Headteacher: Miss N Fowles
Deputy Headteacher: Miss C Budd
Tel: 0121 779 8070
office@chs.solihull.sch.uk

COLESHILL HEATH SCHOOL – ICT and ONLINE SAFETY POLICY

At Coleshill Heath School, we understand that information technology is an essential resource for supporting teaching and learning. Devices combined with utilisation of the internet open up opportunities for pupils to learn about and explore the world in new and engaging ways. Many of these devices already play a part in their day to day home lives and it's important to educate children in using technology safely and effectively.

Whilst the school recognises the importance of promoting the use of information technology throughout the curriculum, we also understand the need to provide safe internet access and encourage appropriate use.

This policy is designed to ensure appropriate and safe use of the internet and all information technology devices throughout school by both pupils and staff. We also hope to encourage a culture of appropriate and safe use in the home environment by providing educational resources to staff and parents and carers using a new online learning platform.

The school is wholly committed to providing a safe learning and teaching environment for all pupils.

Our Vision and Aims

C - Coleshill Heath School is a **caring community**,

H – Offering a **hardworking** and **happy** environment,

S - Enabling children to feel **secure** and enjoy educational success.

Legal Framework

This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation
- Freedom of Information Act 2000

This policy also has regard to the following statutory guidance:

- DfE 'Keeping Children Safe in Education'

This policy will be used in conjunction with the following school policies and procedures:

- Positive Behaviour Policy (including Anti-Bullying and Reasonable use of Force)
- Acceptable Use Policy

Use of the Internet

1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.
2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.
3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:
    1. Access to illegal, harmful or inappropriate images
    2. Cyber bullying
    3. Access to, or loss of, personal information
    4. Access to unsuitable online videos or games
    5. Loss of personal images
    6. Inappropriate communication with others
    7. Illegal downloading of files
    8. Exposure to explicit or harmful content, e.g. content involving radicalisation
    9. Plagiarism and copyright infringement
    10. Sharing the personal information of others without the individual's consent or knowledge

Roles and Responsibilities

1. It is the responsibility of all staff to be aware of possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school. Incidents that arise will be dealt with in accordance with school safeguarding policies.
2. The Governing Body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.
3. The Network Manager is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.
4. The Headteacher will ensure there is a system in place which monitors and supports the Network Manager, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

5. The Network Manager will regularly monitor the provision of e-safety in the school and will provide feedback to the Headteacher.
6. The DSL team will address e-Safety issues according to school safeguarding policies.
7. The Headteacher and Network Manager will review annually or as needed the effectiveness of the e-safety provision, bringing school up to date with current issues and evolving technologies.
8. The Headteacher will review incident logs, either from CPOMS or SENSO alerts as part of the school's duty of care.
9. The Governing Board will evaluate and review this Online Safety Policy on a two-yearly basis, considering the latest developments in ICT and any feedback from staff/pupils.
10. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.
11. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this ICT and Online Safety Policy.
12. All staff and pupils will ensure they understand and adhere to our **Acceptable Use Policy**.
13. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.
14. School will provide relevant e-Safety training to all staff using an online learning platform (National Online Safety).

Online Safety Communication

Successfully communicating information pertaining to online safety to our community is paramount to creating a positive internet and device usage culture.

To achieve this we will:

1. Make this policy and related documents available on the school website.
2. Share this policy and related documents to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated.
3. Display relevant online safety information and displays in all areas where information technology is used.

4. Provide online safety information to parents and carers through social media and school website, the National Online Safety platform, parents' evenings and the school newsletter.

Teaching and Learning

The purpose of technology and The Internet in school is to raise educational standards. Used appropriately, we're able to increase learning, promote pupil achievement, support the professional work of staff and assist in school management.

The Internet is an essential part of life and plays many roles in education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

School Internet access levels will be targeted based on user. Pupil accounts will include age appropriate content filtering, whilst staff levels can be raised to include additional access at the Headteacher's discretion. Pupils will be taught how to behave in an online world and what Internet use is acceptable and what is not. Use of the internet throughout the curriculum should have a clear objective. Internet access will be incorporated into the curriculum to enrich and extend learning activities.

Access levels will be reviewed regularly to reflect changing curriculum requirements. Should a staff member or pupil discover an unsuitable site, the URL (address), time, date and content will be reported to Solihull ICT Development Service, and where appropriate the Headteacher.

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. This will be supported through online safety sessions in school and promotion of online safety values throughout the whole curriculum.

Managing Internet Access

The security of the school information systems will be reviewed regularly. Devices are protected and updated regularly with Windows updates and Virus protection.

Our Internet connection is provided through Solihull Broadband which uses Smoothwall firewall and filtration designed to block harmful, unsafe and inappropriate websites.

Coleshill Heath are a part of the Unity network and domain which includes additional protection through services such as SENSO. Support for our own Network Manager can be obtained from Unity IT services.

Published Content and the School Website

1. The contact details on the school website should be the school address, e-mail and telephone number. Personal contact information for staff will not be published.
2. The Network Manager, under supervision from the Headteacher/Deputy, will take overall editorial responsibility of the website and social media pages and ensure that content is accurate and appropriate.
3. Photographs and other Media that include pupils will be selected carefully. It is the school's responsibility to adhere to parental consent for published photos and media.

Social Networking and Personal Publishing

Social networking sites will be blocked to all users unless approved by the Headteacher. Teacher accounts currently have limited social media access to help with publicising the school. Pupils and other accounts have no access to these sites.

Pupils are advised as part of our curriculum and in particular during computing and PHSE lessons on e-safety, to never to give out personal details that may identify them or their location. This includes real name, address, mobile or landline phone numbers, school, instant messaging (IM) address, e-mail address, names of friends, specific interests and clubs etc. Children will be educated in understanding their responsibilities when using social media and in how to behave in an online world. Should an incident occur it is vital that our children know how to respond and to whom they can share their concerns.

School Technologies

1. Classrooms are fitted with a desktop computer and interactive screen for educational use and to facilitate teaching.
2. School staff where appropriate are provided with a laptop and/or tablet for educational use and their own professional development in and out of school.
3. All staff understand that the Acceptable Use Policy applies to this equipment at all times.

4. To ensure the security of the school systems, personal equipment is currently not permitted to join the school network. Use of Wi-Fi is permitted with installation of a local authority CA certificate.
5. Windows devices that are to be used off site should have a level of encryption in the event a device becomes missing or stolen. This should be reported to the network manager asap.
6. Staff and visitors understand that they should use their own mobile phones sensibly and in line with school policy.
7. Pupils understand that they should ideally not bring mobile phones to school. However, if it is necessary, these should be switched off and handed to the class teacher in the morning who will place them in the classroom safe.
8. Printing in school is managed by papercut and is sent via hold queues, so all users printing must release prints at a physical machine. This stops documents with potentially sensitive information on being seen by pupils or other staff members.
9. School curriculum devices are all managed and securely stored. It is all staff members responsibilities to make sure devices are returned to their respective stores for security, charging and updates.
10. Unauthenticated devices (tablets etc) can be elevated for teacher access by logging in through Smoothwall.

The Educations and Inspections Act 2006 grants the Headteacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Headteacher will exercise this right at their discretion.

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

Staff should not use **personal** mobile phones to take pictures or videos of children. Staff should only use devices which have been provided by the school. Mobile phones are to only be used in designated areas where no children are present.

Children who bring mobile phones to school are required to hand them in to the class teacher every morning and devices are collected at home time.

Coleshill Heath School takes no responsibility for lost or stolen devices.

The Prevent Duty and Online Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the Internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well-being of any pupil is being compromised.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Software updates will be installed regularly on all devices.
- Security strategies will be discussed with the Local Authority and with Unity IT services.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Local Authority can accept liability for the material accessed, or for any consequences of Internet access.

The school will be guided by Solihull policy to provide the best filtering and monitoring that is available. The Deputy Headteacher will ensure that this Online Safety Policy is implemented and its compliance with the policy is monitored.

Handling Online Safety Complaints

- Complaints of Internet misuse will be 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 will be informed of the complaints procedure.
- Discussions will be held with the Local Police Community Officers to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School Online Safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of Online Safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the School Website. The school will also organise Online Safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Professional Conduct Agreement

We acknowledge that practitioners will use digital technologies in their personal and social lives so we require them to sign the following Professional Conduct Agreement to ensure clear boundaries between their home and professional roles.

I agree that through my recreational use of social networking sites or other online technologies that I will:

- Not bring Coleshill Heath or Solihull Borough into disrepute.
- Observe confidentiality and refrain from publicly discussing or posting any issues relating to work.
- Not share or post in an open forum, any information that I would not want children, parents/carers or colleagues to view.
- Set privacy settings to block unauthorised access to my social networking page and to restrict those who are able to receive updates.
- Keep my professional and personal life separate by not accepting children as 'friends', and refraining from using social media during school hours.
- Consider how my social conduct may be perceived by others and how this could affect my own reputation and that of Coleshill Heath School.
- Either avoid using a profile photograph or ensure it is an image I would be happy to share with anyone.
- Report any known breaches of the above.

I understand I am in a position of trust and that my actions outside of my professional environment could be misinterpreted by others. I am conscious of this when sharing information publicly with other people.

Name: _____ Signature: _____

Date: ___/___/___

COLESHILL HEATH SCHOOL
EVERY CHILD, EVERY DAY

Policy Name:	**ICT and ONLINE SAFETY**
Staff Responsible:	Mr M Abbott – Network Manager
Governor Responsible:	Curriculum and Standards (C&S) / Scrutiny and Outcomes (S&O) Committee
Date for Review:	June 2024
Signed Headteacher:	Miss N Fowles
Signed Chair of Governors:	Mrs M Fitter
Ratified:	Full Board – 13th September 2022