

Online Safety Policy

Date established by governing body

Autumn Term 2024

Date for full implementation

Immediately

Date for review

Autumn Term 2026

RATIONALE

At Cleaswell Hill School we believe that computing and the internet are valuable resources to both teachers and pupils and can help raise standards. Recognising the dangers and planning the use of suitable resources is vital to safeguard children in our school. Our aim is to promote safe use of ICT and online resources, through the continual development of pupil, parent/carers, governors, teaching assistant and teacher awareness.

WHY IS ONLINE SAFETY IMPORTANT?

This policy document aims to outline how we educate children and parents/carers to use the internet safely.

Children working online in school or at home will be supported to understand and recognise the risks they face and will be equipped with strategies to deal with issues as they arise.

Teachers, children and parents/carers will receive information to highlight factors they should consider when using computing equipment and the Internet.

Pupils have access to technologies in a range of locations such as school, home, and through mobile phones to portable games consoles.

At Cleaswell Hill we develop an awareness of online safety through the use of our Acceptable Use Policy (AUP), digital safety rules, curriculum and focused events, for eg. Safer Internet Day.

SCHOOL STAFF

Due to continual developments in computing, planning and practice need to be assessed and changed to suit the needs of the children in our school. At Cleaswell Hill it is essential that the staff are briefed on procedures that will allow them to deal with discussions about children's internet use and online presence.

Staff receive the necessary training, advice and signposting in order to combat difficulties which children in their class may face.

Advice and training may be obtained from outside agencies, advisors and documents such as;

- Teaching Online Safety in Schools - DFE June 2023
- Keeping Children Safe in Education - DFE 2024

In order to continue to develop strategies to enhance online safety in our school, the computing curriculum subject lead / CEOP Ambassador and Designated Safeguarding Lead will regularly attend online safety training and keep their skills and knowledge updated.

Key information will be fed back to staff through briefing notes, policy documents and staff development sessions and Governor Monitoring Reports.

The school ethos encourages trust between staff, pupils and parents/carers. As teachers it is part of our role that we safeguard children in our care and educate them about how to safely use ICT equipment and the internet both in and out of school.

Each academic year, all staff members are required to sign that they have read Keeping Children Safe in Education (2024). In signing this and in accepting the AUP, staff members accept that they

understand and agree to action these policies and also that the school can monitor network and internet use to help ensure staff and pupil safety.

At Cleaswell Hill an effective approach to online safety empowers our school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users;
- Conduct: personal online behaviour that increases the likelihood of, or causes harm; and
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Staff will be briefed on procedures that define how inappropriate or illegal ICT use is reported to the School Leadership Team. SLT will follow set procedures (see below) and investigate incidents with care and attention. Staff will be briefed on the dangers of mismanagement of ICT, for example, the potential for children to view inappropriate images if a search engine is used during a lesson without prior planning.

Staff are given a personal work email account. Staff must use '2 factor verification' when logging into email accounts on any device.

Good communication is vital in a large school and is key to the smooth running of Cleaswell Hill. Staff members may be required to use school telephones, which is essential to the safeguarding of children. The use of personal mobile phones is prohibited during teaching time when phones should be switched off. We have mobile phones for use on visits. These are locked securely in the school office when not being used. Personal mobiles must not be used to take or store images of children.

Pupils who need to bring mobile phones to school for safety reasons when travelling to and from school hand the phone into the Main Office. The pupil's phone is stored here for the duration of the day and collected by children on their way home.

ROUTES TO ONLINE SAFETY

Open access to the internet has become an integral part of children's lives. A growing danger is presented by the ease of uploading material to the internet. We are aware that pupils' may frequently use social media at home.

Social networking sites allow children to set up an account and create a web page in minutes. Online safety will be introduced to children through a whole school approach, as appropriate, every academic year.

Through planned lessons, children will develop a better insight into the meaning of 'E-Safety' or online safety within the context of school and home.

A curriculum framework has been adopted; [UKCIS Education for a Connected World](#)

A series of web-links, guidance and advice are shared with parents via the school website. School signpost parents as often as possible to help awareness.

Staff are prepared to tackle online safety issues throughout the school year. This will mean adapting curriculum planning to online safety situations as they arise.

Any incidents should be passed on to the DSL and Computing Curriculum Lead following the flow chart in section 10.1. SENSO is used to monitor input on all school devices. Incidents are investigated and recorded through CPOMs.

Raising awareness among children and young people of the risks associated with internet and apps whilst not wishing to alarm anyone, is a responsibility for all members of staff. Staff will be asked to review and refine their practices to ensure pupils are safe.

Through online safety teaching, we will educate children about the dangers of accessing sites through links sent to them, in-app extras and online gaming.

We will highlight the need to seek advice from teachers or family members. Pupils will be told not to upload photographs or videos of themselves or other pupils. They must not publish personal information, such as their address or contact details.

PARENTAL INVOLVEMENT

Working alongside parents/carers is vital when promoting online safety, as children can spend a lot of time using ICT in their homes, such as internet browsing, chat rooms, messenger facilities, games consoles, etc.

Providing parents/carers with the appropriate information regarding safeguarding their children is essential.

Key areas to be focused on will be;

- Mobile phones
- Selfies
- Internet grooming
- Gaming websites or consoles that can be attached to the Internet
- Social networking sites
- Cyberbullying
- Chat forums or blogs

Parents/carers will be made aware of how they can report incidents using the 'Report Abuse' facility on the school website and 'Think You Know' homepage.

Parents will be provided with information about how we promote online safety in school and the rules we will implement.

IDENTIFYING VULNERABLE GROUPS

The majority of pupils have access to mobile devices. The use of smart devices and handheld games consoles outside school is common place. All pupils will be supported to understand risk and to use these devices safely.

We are aware that many of the children will not necessarily understand the term "safety". Children will take part in assemblies where safety will be addressed through multimedia presentation provided by CEOP 'Think U Know' site, which provides suitable material for varying age ranges. We also have staff trained in the delivery of NSPCC Speak Out, Stay Safe Programme and this is delivered to pupils as part of the PSHEE curriculum.

As part of the computing/digital safety curriculum, teachers will be required to teach children safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. When children progress in their understanding, guidelines are adjusted and changed. Children need to learn how to apply strategies that will help them to avoid certain "risks". Visual aids will be displayed in the classrooms and areas where children come into contact with ICT, to promote safety. There are certain aspects of the above that are particularly challenging for our pupils.

Children will clearly have individual needs that present different issues when teaching online safety but some common difficulties may be;

- developing social understanding of safety and so may relate better to strategies used with younger children
- finding it hard to apply the same rules in different situations
- Safety principles relying on children being able to explain what happened or to ask for help
- Blurred lines between fantasy and reality
- Poor recall and difficulties with learning through experience.

Appropriate resources in order to promote safety, including visual aids, websites and advice on how to develop children's awareness of how to use the Internet safely, will be available.
Adults need to plan group interactions carefully when raising awareness of internet safety.

The Designated Safeguarding Lead (DSL) is Karyn McMahon. In her absence it is Julie Brown or Emma Dunn. David Evans leads the Computing Curriculum Subject area and is the school CEOP Ambassador.

USING THE INTERNET TO SUPPORT LEARNING

Websites and apps are essential to teaching. Staff members are encouraged to use safe, purposeful sites and apps that are beneficial to learners.

Through the use of UK Safer Internet; ThinkUKnow; NSPCC; SWGfL advice, websites are recommended that contain suitable content to assist teaching and learning.

We recognise that there is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery.

For most of our pupils, the greatest risk is through inadvertent access. Fast WiFi speeds means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. In the unlikely event of this happening in school, teachers will be advised to;

- Tell children to minimize the screen immediately
- Do not navigate away from the screen
- Talk to children about what has happened and reassure them they are not in trouble
- Later investigate the history of the sites visited to get details of the inappropriate site and how the child got there
- Report the incident using the appropriate form
- In light of potential problems when accessing Internet sites or search engines, pupils are not permitted to use the internet or an ipad in school unless they are supervised by an adult.

CURRICULUM PLANNING

Good planning and preparation is critical in ensuring a safe starting point for online safety teaching.

Online safety is planned as part of the computing curriculum. Using the framework above to plan for appropriate online safety themes.

Teachers also teach online safety 'incidentally' when issues, questions and incidents arise throughout the academic year.

RESPONSE TO AN INCIDENT OF CONCERN

Web based technology provides children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school.

We recognise the importance of considering the risk associated with technology our children come into contact with.

At Cleaswell Hill we develop the skills that children and young people need when communicating and using these web based technologies properly, while keeping safe and secure, and acting with respect for other users.

Our school website is populated with resources to aid children and parents when reporting safety concerns.

Teachers are our first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will provide guidance to help staff determine what action they can take within the school and when to escalate concerns.

What Does Electronic Communication Include?

Internet collaboration tools: social networking sites and blogs
Internet Research: web sites, search engines and Web browsers
Mobile Phones and personal digital assistants (PDAs)
Internet communications: e-Mail and instant messaging (IM)
Webcams and videoconferencing

What Are The Risks?

Receiving inappropriate content
Publishing inappropriate content
Predation and grooming
Online gambling
Requests for personal information
Misuse of computer systems
Viewing 'incitement' sites
Publishing personal information / images
Bullying and threats
Hacking and security breaches
Identity theft

How Do We Respond?

Northumberland Strategic Safeguarding Partnership (NSSP) have provided guidance on how incidents should be reported.

The expected response will be to report incidents to the DSL in school, who will then refer details of the incident, as appropriate, to the lead agencies involved in safeguarding children. The flowchart on this page is the approach used to investigating an incident of concern.

Staff are made aware of supporting documents to assist schools when responding to incidents.

Dealing with referrals

We are aware of the potential indicating factors that a child is vulnerable to being radicalised or exposed to extreme views, including peer pressure, influence from other people or the internet, bullying, crime and anti-social behaviour, family tensions, race/hate crime, lack of self-esteem or identity, prejudicial behaviour and personal or political grievances.

In the event of prejudicial behaviour the following system will be followed:

All incidents of prejudicial behaviour will be reported directly to the SLT or the Head Teacher. All incidents will be fully investigated and recorded in line with the Behaviour and Communication Policy and records will be kept in line with procedures for any other safeguarding incident.

Parents/carers will be contacted and the incident discussed in detail, aiming to identify motivating factors, any changes in circumstances at home, parental views of the incident and to assess whether the incident is serious enough to warrant a further referral. A record of this meeting is kept alongside the initial referral on CPOMS.

A member of the SLT will follow-up any referrals for a period of weeks after the incident to assess whether there is a change in behaviour and/or attitude.

A further meeting with parents would be held if there is not a significant positive change in behaviour. If deemed necessary, serious incidents will be discussed and referred to the local children's social care team.

In the event of a referral relating to serious concerns about potential radicalisation or extremism, the school will also contact preventmailbox@northumbria.pnn.police.uk

NCC Information Security Event Report form would be completed to report events which required further investigation. School keeps a log of incidents.

INFORMATION SYSTEMS INTEGRITY AND SECURITY

We have a responsibility to ensure that our capital investment in Computing is protected and secured. Changes or modifications to the hardware, network wiring, or software configurations will be completed by designated support personnel.

At Cleaswell Hill School the Admin network has access to the Northumberland County Council intranet. A firewall is in place and prevents access from external sites to the curriculum network.

Curriculum devices are filtered by Senso (provided and maintained by NCC).

Senso sessions are created for individual users based on their network accounts. Senso provides global filtering for schools in Northumberland.

The broadband link is provided by the Northumberland County Council.

Microsoft System Centre Endpoint Protection is installed on all Curriculum Windows 10 devices. This comprehensive software is managed by the school's SCCM installation.

SENSO also monitors the web. SENSO runs in the background of Curriculum Windows 10 devices in school. It enables a key logging system, a weekly report is generated. This report can be seen by the designated personnel; Mike Jackson (Head teacher) Karyn McMahon (DSL), David Evans (DDSL).

Any queries about the weekly report or incidents are followed up and staff are involved when necessary.

DISASTER RECOVERY SYSTEM

The three Hyper-V hosts back their virtual machines up to the NAS device located in the Server Room during every night. They also back up to the NAS device located in the cabin every week. These backups are encrypted.

MAINTENANCE

NCC Admin devices are maintained by NCC Information Services Schools Team.

Curriculum devices are maintained in-house.

Related documents:

Acceptable Use Policy

Safeguarding & Child Protection Policy

Computing Policy

Equality Objectives
Behaviour is Communication Policy
Tackling Extremism & Radicalisation
PREVENT Strategy HM Gov
Keeping Children Safe in Education DfE 2024
Working Together to Safeguard Children HM Gov 2023

Author: Karyn McMahon/David Evans

Headteacher: Mike Jackson

Chair of Governors: Tim Chrisp

Date: Autumn 2024