

The Cliff Federation

E-Safety and Acceptable Usage Policy

<u>Policy Information</u>			
Status:	Statutory	Reviewed by:	Full Governing Body
Cycle of Review:	Annual	Policy Ratified:	November 2025
Signed as accepted:			

The Headteacher is also the E-Safety Coordinator.

Contact details:

Senior lead for safeguarding and child protection and Online safety co-ordinator

Name: Mrs Kerry Lakin Email: Kerry.lakin@hemswellcliff.lincs.sch.uk

Named Governor Responsible for Online Safety

Name: Mrs Sally Cowell Email: Sally.Cowell@willoughton.lincs.sch.uk

NSPCC Helpline 0808 800 5000

Purpose of Policy

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in the Cliff Federation's activities

Introduction

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

ICT in the 21st Century 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 **safe** use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

We also recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges.
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
- we have a responsibility to help keep children and young people safe online, whether or not they are using the Cliff Federation's network and devices.

- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently, the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs
- AI (artificial intelligence)

Whilst exciting and beneficial both in and out of the context of education much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At the Cliff Federation, we understand the responsibility to educate our pupils on E-Safety Issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement –Appendix One (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring and Filtering

Each school's Internet provider logs all Internet activity. That provider may monitor these logs. Ark (at HCPS) provide a weekly report of Internet Activity logs and share with the Subject Lead and Headteacher for review as needed. KCSiE (2023 Update) sets out clear expectation that School is monitoring internet use in order to minimise the risks to children.

A breach or suspected breach of policy by a pupil will be dealt with in reference to the school's behaviour policy.

E-Safety

We will seek to keep children and young people safe by:

- appointing an online safety coordinator (the Headteacher).
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults.
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others by ensuring e-safety is an integral part of all relevant computing units.
- supporting and encouraging parents and carers to do what they can to keep their children safe online, including by providing 'Wake up Wednesday' e-safety information from National Online Safety and by signposting relevant courses and information sources.
- developing an online safety agreement for use with young people and their parents or carers, a signed copy of which is kept in the pupil's file. (A copy is given at the end of this policy)
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person in line with our Child Protection and Safeguarding Policy.
- reviewing and updating the security of our information systems regularly with the support of our IT providers.
- ensuring that usernames, logins, email accounts and passwords are used effectively.
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate in line with current GDPR guidance.
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given in line with our 'Use of personal images policy.'
- providing supervision, support and training for staff and volunteers about online safety.
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

E-Safety encompasses the use of new technologies, Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety policy will operate in conjunction with other policies including those for Security.

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
Internet use enhances learning

The school Internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils.

Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils are taught how to evaluate Internet content.

The school ensures that the use of Internet derived materials by staff and pupils comply with copyright law.

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with Central IT.

E-mail

- Pupils may only use approved class e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Staff should follow advice given in order to protect school from potential cyber-security breaches, including being vigilant against possible phishing emails or data breaches.

Published content and each school's web site

The contact details on the Web sites are the school address, e-mail and telephone number. Staff or pupils' personal information are not published.

The head teacher takes overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils are selected carefully and do not enable individual pupils to be clearly identified.

Pupils' full names are not used anywhere on the Website or Blog.

Written permission from parents or carers is obtained, on admissions and contact forms, for photographs of their child to be used on the school Web site / Facebook page / Twitter / Class Dojo and in the local press.

Social networking and personal publishing

The school blocks/filters access to social networking sites.

Newsgroups are blocked unless a specific use is approved.

Pupils are advised never to give out personal details of any kind that may identify them or their location.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse).
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation.
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- child protection and safeguarding
- procedures for responding to concerns about a child or young person's wellbeing
- dealing with allegations of abuse made against a child or young person
- managing allegations against staff and volunteers
- code of conduct for staff and volunteers
- anti-bullying policy and procedures
- Use of personal images policy and GDPR guidance.

Primary Pupil Acceptable Use Agreement / ESafety Rules

- I will only use ICT in school for school purposes
- I will only use my class email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carers contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher



Capper Avenue, Hemswell Cliff, Gainsborough, Lincs, DN21 5XS,
Tel. 01427-668383
enquiries@hemswellcliff.lincs.sch.uk
Website: www.hemswellcliff.lincs.sch.uk
Headteacher: Mrs K Lakin

Dear Parent/ Carer

ICT including the Internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-Safety rules with your child/ren and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact Mrs Lakin.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂

Parent/Carer signature

We have discussed this document with(child/ren's name/s) and we agree to follow the E-Safety rules and to support the safe use of ICT at Hemswell Cliff Primary School.

Parent/Carer Signature:

Class

Date