Ellingham VC & Woodton Primary Federation

WHOLE SCHOOL POLICY FOR

Online Safety

Date Reviewed:	Agreed by Governors:	Date for Next Review:
January 2024		January 2025

Our vision is to love our neighbour, enabling everyone to flourish and to reach their full potential.

Inspire Challenge Nurture

Online Safety Policy

The school has a Designated Online Safety Leader (Ali Snelling), who is responsible for reviewing and updating this policy. They work in collaboration with members of the SLT in order to ensure this policy meets the ever-changing issues relating to the internet and its safe use.

The Online Safety Policy has been written by the school, incorporating points from the Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education', its non-statutory guidance 'Teaching Online Safety in Schools' and a number of other carefully selected sources. Key documents in school that inform this document and have, in turn, been informed by this document include the Safeguarding Policy and the Child Protection Policy. This policy has been agreed by the senior leadership team and approved by the Governing Body. It will be reviewed regularly and updated at least annually. Changes will be made immediately if technological or other developments require it.

Online Safety Risks

The Department for Education published an updated version of 'Keeping children safe in education' in 2023. It states the following:

- *All staff should be aware of indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of home and online. Exercising professional curiosity and knowing what to look for is vital for the early identification of abuse and neglect so that staff are able to identify cases of children who may be in need of help or protection.*

- *All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content*

- *It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns 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 content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.*

  ***Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*

  ***Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and*

  ***Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

The importance of staff understanding the role that children can plan in abusing other children is highlighted in the document:

- *All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school or college and online. All staff should be clear as to the school's or college's policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.*

Please see the school's Safeguarding Policy for more information.

Filtering and Monitoring

Statutory guidance from the 2023 update of KCSIE dictates the following:

- *Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.* Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

An addition to this year's KCSIE update includes specific expectations around filtering and monitoring in schools and directs education settings to the updated document 'Meeting digital and technology standards in schools and colleges':

- *To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:*
    - *identify and assign roles and responsibilities to manage filtering and monitoring systems.*
    - *review filtering and monitoring provision at least annually.*
    - *block harmful and inappropriate content without unreasonably impacting teaching and learning.*
    - *have effective monitoring strategies in place that meet their safeguarding needs.*

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Additional guidance on filtering and monitoring can be found at: UK Safer Internet Centre: "appropriate" filtering and monitoring https://www.saferinternet.org.uk/advicecentre/teachers-and-school-staff/appropriate-filteringand-monitoring South West Grid for Learning (swgfl.org.uk) have created a tool to check whether a school or college's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).

- *Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and 36 smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how*

> *this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

In line with DfE guidance, the Federation has appropriate filtering and monitoring systems in place. The school's broadband connection is provided by Schools Broadband. The filters in place include lists of illegal sites/inappropriate sites that cannot be accessed. Use of the web through Schools Broadband services is monitored and traceable by the network administrators: JC Comtech, including alerts provided to the senior DSL (Dawn Read, Headteacher) in the event of access to websites that may contain inappropriate content.

Searches using the school's network are monitored. The school uses Schools Broadband to notify the senior DSL of any inappropriate searches or searches which then result in accessing a site with potentially inappropriate content.

From time to time websites can be blocked even though there are no obvious threats or dangers. Once these have been checked thoroughly by a member of staff, they can contact the JC Comtech Helpdesk to notify them that a website is suitable for educational purposes. This can be done at: jccomtech.deskpro.com. Staff should ensure that they use their school email account for this purpose.

Online Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential Online Safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.

Online Safety education will be provided in the following ways:

Online Safety Training for Staff and Governors

At Ellingham VC and Woodton Primary Federation we ensure that all teaching and non-teaching staff can recognise and are aware of Online Safety issues. All staff take responsibility for promoting online safety. The 2023 update to KCSIE states:

> *Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description.*
>
> *Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction. This training should equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding. Their training should be regularly updated.*

DSLs deliver annual safeguarding training, which includes Online safety, where information is shared with staff about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding (for example, the Prevent strategy).

Online Safety Support for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

As part of the school's weekly newsletters, there is an 'Online Safety' section. This offers information and links to further guidance for parents to help them understand the importance of online safety. The Online Safety section of the newsletter is bespoke to issues arising in school, but also to relevant online safety issues we feel parents/carers need to be aware of.

Online Safety within the Curriculum

With regard to teaching Online Safety in school, the 2023 KCSIE update states:

> *Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.*

Using searchable cached sites such as Espresso provide a completely safe environment for children to conduct research. However, limiting access will not protect children and educate them to be safe on the internet. Therefore, it is vital to provide opportunities for children to conduct safe searches.

Accessing and interacting with the internet is a key aspect of many users' reasons for having an internet connection. Simply preventing the children from using internet is not preparing them for the real world (including for use at home). Therefore, online safety is implicitly taught throughout school and referred to whenever a unit of work requires use of the internet.

An Online Safety lesson is delivered at the beginning of each half term using Project Evolve (https://projectevolve.co.uk/), and each half term there is a focus for the lesson.

Autumn 1	Autumn 2	Summer 1
Self-Image and Identity	Online Relationships	Managing Online Information
Spring 1	**Spring 2**	**Summer 2**
Online Reputation	Online Bullying	Privacy and Security

Cyberbullying

The National Children's Bureau (2016) defines cyberbullying as:

> *'any form of bullying that is carried out through the use of electronic media devices, such as computers, laptops, smartphones, tablets, or gaming consoles', and adds that an instance of this would be 'an aggressive, intentional act carried out by a group or individual, using mobile phones or the internet, repeatedly and over time against a victim who cannot easily defend him or herself'.*

This policy recognises the following as examples of cyberbullying though the list is not exhaustive:

- Bullying by text, calls, video, email or through social media on any device capable of sending communications.

- The use of technology to cause distress, fear or humiliation.
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social media sites and apps.
- Using digital devices to message others inappropriately.
- Hacking online accounts and/or creating fake accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms and through social media sites and apps.
- Impersonating others on social media sites and apps by creating fake profiles or hijacking accounts

Ellingham VC and Woodton Primary Federation embraces the advantages of modern technology in terms of the educational benefits it brings. However, the school is mindful of the potential for bullying to occur. Central to the School's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'. The school also recognises that it must take note of bullying perpetrated outside school which spills over into the school

Cyberbullying is generally criminal in character. The law applies to cyberspace as outlined below:

- It is unlawful to disseminate defamatory information in any media including internet sites.
- Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

Ellingham VC and Woodton Primary Federation educates its pupils about the serious consequences of cyber-bullying and will, through the PSHE and computing curriculums and assemblies, continue to inform and educate its pupils in these fast-changing areas. Ellingham VC and Woodton Primary Federation trains its staff to respond effectively to reports of cyberbullying or harassment and has systems in place to respond to it.

Whilst education and guidance remain at the heart of what we do, Ellingham VC and Woodton Primary Federation reserves the right to take action against those who take part in cyberbullying. All bullying is damaging but cyberbullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts. Ellingham VC and Woodton Primary Federation supports victims and, when necessary, will work with the police to detect those involved in criminal acts. Ellingham VC and Woodton Primary Federation will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, either inside or outside of school.

All members of the School community are aware they have a duty to bring to the attention of the Head teacher/DSL any example of cyber-bullying or harassment that they know about or suspect.

Links with other policies

This policy should be read alongside Ellingham CE VC and Woodton Federation policies and procedures on child protection and safeguarding. More information about safeguarding and child protection can be found on the school website http://www.ellinghamandwoodton.co.uk/

This online safety policy is linked to our:

- Safeguarding Policy, including Child Protection
- Behaviour and relationships policy
- Staff discipline and conduct policy
- Data protection policy and privacy notices
- Staff code of conduct
- Home School Agreement
- Acceptable Use Agreements (See appendices)

Appendix 1

Primary Pupil Acceptable Use Agreement / Online Rules

- I will only use ICT in school for school purposes
- I know that if I bring a mobile device into school, it must be handed in to the school office on arrival and I will collect it at the end of the school day.
- 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 look for, save or send anything that could be unpleasant or unkind. 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.
- 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 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/carer 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
- I will only access age appropriate sites and APPs
- I will only use my class email address or my own school email address when emailing (where applicable)
- I will only open email attachments from people I know, or who my teacher has approved

Name___________________
Class ___________________
Date ____________________

Appendix 2
Letter to parents/carers about Acceptable Use Agreement

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 online rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the school office for further support.

It is also important that at home you have the appropriate systems in place to protect and support your child/ren. Please ensure that there are filters set to support this, if you need any help with this, please contact us.

Yours Sincerely,

Miss Read
Headteacher

We can confirm that we have discussed this document with ……………………………………………...... (child's name) and we agree to follow the online rules and to support the safe use of ICT at Ellingham VC and Woodton Primary Federation.

Parent/ Carer Signature ……..……………………………………………….

Class …………………………………. Date ……………………………

Appendix 3
Acceptable Use Agreement (staff & governors)

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Board
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on Pupil Asset) is kept secure and is used appropriately. (Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Board).
- Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the school
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes on school equipment, unless previously agreed with the headteacher
- Images will not be distributed outside the school network without the permission of the parent/ carer – permissions are sought at the beginning of each year.
- I will support the school approach to online safety
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's Online Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and if previously agreed with the headteacher
- I understand this forms part of the terms and conditions set out in my contract of employment

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature ………………………………… Date ……………………
Full Name …………………………………………….. Job title ………………