Ellingham VC & Woodton Primary Federation

WHOLE SCHOOL POLICY FOR

Online Safety

Date Reviewed:	Agreed by Governors:	Date for Next Review:
January 2025	January 2025	January 2026

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

RESPECT	CHALLENGE	INSPIRE	RESILIENCE	NURTURE	ASPIRATION

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.

Every half a term, a parent newsletter is sent to share which area of online safety we have taught in class. This offers information and links to further guidance for parents to help them understand the importance of online safety.

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

Pupil Acceptable Use Agreement
2024-2025

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules, I might not be allowed to use a computer/tablet

Signed (child): ....

Signed (parent): ....

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,

Mrs Thomas
Executive 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)

Staff Acceptable Use Agreement
2024-2025

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include) a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: ....
Signed: ....
Date: ....