Ellingham VC & Woodton Primary Federation

WHOLE SCHOOL POLICY FOR

Online Safety

Date Reviewed:	Agreed by Governors:	Date for Next Review:
October 2022	October 2022	October 2023

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

Inspire Challenge Nurture

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/

Aims

Our federation aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum Computing

Summary of key online safety requirements and within KCSIE 2022:

- DSLs continue to have overall responsibility for online safety and this cannot be delegated. They can be supported by appropriately trained deputies and liaise with other staff on matters of online safety.
- DSLs should continue to be able to evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff should continue to be provided with online safety training at induction and as part of regular child protection training and updates.
- Part 5 continues to recognise that child on child sexual violence and sexual harassment can occur on and offline.
- Additions have been made to content relating to Child Sexual Exploitation and Child Criminal Exploitation to recognise the role technology can play.
- An additional section has been added to part one to help staff make the link between mental health concerns and safeguarding issues. Whilst online safety is not specifically addressed, the section signposts to guidance and resources where online safety is explored.
- Links to additional or updated resources have been included to support schools and colleges in teaching online safety to all learners as part of providing a broad and balanced curriculum, including as part of the requirements for Relationships Education and Relationships and Sex Education.
- Additional information is available on how to support keeping children safe online when they are learning at home within annex B.

- Content relating to 'upskirting' has been updated to reflect that anyone of any gender can be a victim.
- Additional links to new guidance and resources related to online safety have been added throughout and particularly in annex B & C.

Roles and responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety as part if safeguarding monitoring.

Headteacher and The Designated Safeguarding Leads (DSLs)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Addressing any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately; in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services as necessary
- Providing regular reports on online safety to the governing body

JC Comtech (ICT Support)

JC Comtech are responsible, in discussion with the headteacher and Computing Lead for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see appendices 1, 2 & 3)
- Ensuring that pupils follow the school's terms on acceptable use (see appendix 1)
- Working with the Headteacher and DSLs to ensure that any online safety incidents are logged (see appendix) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff of any concerns or queries about online safety
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (see appendices 1 & 2)

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. We revisit online safety every term.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour online
- Identify a range of ways to report concerns online
- The safe use of social media and the internet

The school will also use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Types of Online Safety

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

1. **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
2. **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.

3. **conduct:** 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
4. **commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Supporting parents with online safety

The school will raise parents' awareness of internet safety in letters and with other communications home, and in information via our website. This policy will also be shared with parents via the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with a the headteacher or a DSL.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power (See also the school behaviour policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will:

- Ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- Ensure that pupils know how they can report any incidents, including where they are a witness rather than the victim.
- We will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The Headteacher and DSLs will consider whether the incident should be reported to the police if it involves illegal material and will work with external services when necessary.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2).

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school.

Some of the older children walk home on their own and therefore may need to bring a phone into school. These mobile devices need to be handed into the school office for the school day.

Mobile devices are not permitted to be used by children during the school day.

Staff Online Safety

Training

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

All staff members will receive regular training, as part of the core safeguarding training. This will include: safe internet use, online safeguarding issues (including cyber-bullying) and the risks of online radicalisation.

In addition to this staff members will receive up to date information through regular catch up meetings, via emails and staff meetings.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Staff using work devices outside school

Staff members using a work device outside school must:

- Not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix.
- Ensure that their work device is secure and password-protected, and that they do not share their password with others.
- Take all reasonable steps to ensure the security of their work device when using it outside of school.
- Use USB devices that are encrypted.
- Seek advice from JC Comtec and inform the headteacher if there are any concerns over the security of their device.
- Only use work devices solely for work activities

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Links with other policies

This online safety policy is linked to our:

- Safeguarding Policy
- Behaviour policy
- Staff discipline and conduct policy
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Primary Pupil Acceptable Use Agreement / Online Rules

- I will only use ICT in school for school purposes
- 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 not bring a Smart Watch to school because I am not allowed to wear one during the school day
- 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 e-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 (including smart watches) 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 ……..