Tutshill C of E Primary School

Woolaston Primary School

Forest Edge Federation

Governing Board

E-Safety Policy

Signed: _____

Chair of the Governing Board

Date: September 2024

Review: September 2026

Contents:

1.0 Introduction

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage.

2.0 Purpose

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children is paramount when adults, and children are using the internet or using school iPads.
- 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.
- support pupils and staff to identify the potential safeguarding risks when accessing content and communicating with others online

This policy applies to all staff, volunteers, children and young people and anyone involved in Forest Edge Federation activities. This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

3.0 Aims

At Forest Edge Federation 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.
- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all our pupils are protected from potential harm online
- we have a responsibility to help keep children safe online, whether or not they are using the schools network and devices
- 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
- working in partnership with children, their parents, carers and other agencies is essential in promoting their welfare and helping stay safe online.

4.0 Roles and Responsibilities

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE. Teachers translate these standards appropriately for all matters relating to e-safety.

Designated Safeguarding Lead

- has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place
- should 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.

- ensures safeguarding policies specifically address online safety, especially with regards to appropriate filtering and monitoring on school devices and school

networks, child-on-child abuse, relationships on social media and the use of mobile and smart technology.
- has overall responsibility for online safety,
- ensures all staff, including governors receive appropriate and up-to-date online safety information and training at induction, and as part of regular child protection training and updates
- share information with any new school if there have been any online safety concerns.
- understands that children with special educational needs, disabilities or health issues, or those who are LGBT or are perceived as LGBT can be at increased risk online.
- implements a culture and ethos which facilitates conversations with staff in relation to online matters that may have implications for the safeguarding of children.

Senior Leaders
The senior leadership teams will:

- ensure they have appropriate filtering and monitoring systems in place and regularly review their effectiveness
- be aware how to escalate concerns with filtering and monitoring systems.
- ensure recruitment processes are transparent and ensures that shortlisted candidates are made aware that online searches may be done as part of due diligence checks.
- write and update the staff code of conduct to ensure all staff know the expectations regarding professional conduct online.
- ensure appropriate precautions and action are taken to ensure information held electronically is kept, stored and transferred in accordance with data protection legislation.
- provide advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.
- be aware of how to respond appropriately to incidents involving harmful online challenges and online hoaxes.
- share online safety messages shared with staff and parents/carers that are appropriate and up-to-date and reflect the full range of risks children could encounter online in terms of content, contact, conduct and commerce using resources from known and recognised organisations, for example, NSPCC, NCA-CEOP, Childnet, Internet Matters etc.
- carry out an annual review of their approach to online safety, supported by an annual risk assessment which considers and reflects the risks their learners face.
- liaise with Focus Networks/ LA to ensure the school ICT infrastructure is secure.

All Staff
All staff will:

- attend appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- teach children about online safety, including as part of statutory Relationships and Sex Education (RSE) and should recognise that a one size fits all approach may not be appropriate, and that a more personalised or contextualised approach may be needed for more vulnerable children e.g., victims of abuse and SEND, may be needed.
- know how to raise concerns with the filtering and monitoring systems that are in place.

- recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online and use My Concern to record and report concerns.
- recognise online safety issues as part of their safeguarding responsibilities.
- understand the expectations, applicable roles, and responsibilities in relation to filtering and monitoring in place on school devices and the school network.
- understand that technology is a significant component in many safeguarding and wellbeing issues and that children are at risk of abuse and other risks online as well as face to face.
- recognise that technology can play a key role within child-on-child abuse concerns and that children may 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.
- read the policies and procedures relating to responding to online safety concerns, including online child-on-child abuse issues.
- be aware that children may not feel ready or know how to tell someone they are being abused; this is especially likely to be the case where abuse takes place online.
- know that online safety concerns should be reported to the DSL or a deputy.
- understand that bullying can take the form of cyber-bullying
- recognise consensual and non-consensual sharing of nude and semi-nude images and/or videos is a safeguarding issue and will respond appropriately to concerns.
- read the following policies every year and sign to say they have understood them:
    - school safeguarding policy
    - staff code of conduct
    - acceptable user policy
    - e-safety policy
- recognise the impact and complications social media can bring when responding child on child sexual violence and harassment concerns.
- understand the role of the internet as a tool for radicalisation and in the potential accidental and deliberate exposure to extremist views and content online.

Governing Board

Governors will:

- ratify this policy and review its effectiveness.
- attend appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- understand their strategic role and responsibilities regarding online safety
- ask appropriate questions to assure themselves that online safety policies and procedures are in place in their setting, and that they are effective and support the delivery of a robust whole school approach to online safety.
- take a proportionate risk-based approach to the level of information regarding e-safety and acceptable use that is provided to temporary staff, volunteers, and contractors, however when it comes to the safer use of technology, this may be necessary depending on the context.
- ensure staff to undergo regular updated safeguarding training, including in relation to online safety and for children to be taught about safeguarding, including in relation to online safety
- ensure that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole federation safeguarding approach and wider staff training and curriculum planning.
- make informed decisions regarding the safety and security of the internet access and equipment available within or provided by the school ensuring the welfare of children is paramount. Ensure any decisions regarding filtering and monitoring systems are

taken from a safeguarding, educational and technical approach and ensure that filtering and monitoring decisions are justifiable and documented.

Acceptable Use

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, all staff are required to read this policy annually and sig an agreement before being given access to school systems.

The Acceptable Use Policy (AUP) is revised annually and amended accordingly in the light of new developments and discussions with the children which take place at the time.

Parents and pupils also sign acceptable use agreements and these are kept on file in the classroom.

5.0 Teaching and learning

Why the internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.
- Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Staff model safe and responsible behaviour in their use of technology during lessons.

Teachers remind pupils about their responsibilities through an end-user Pupil Acceptable Use Agreement

We believe that internet use will enhance learning and will be used in the following ways:

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content to the computing lead. This can be done anonymously, or in person, and will be treated in confidence.
- The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience.

6.0 Managing internet access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the LA and Focus networks.

Email

- Pupils may only use approved schools accounts for email.
- Pupils must immediately tell a teacher if they receive an offensive email.
- In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- The school will consider how emails from pupils to external bodies are presented and controlled.
- The forwarding of chain letters is not permitted.

The school:

- Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account.
- Does not publish personal email addresses of pupils or staff on the school website.
- Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

7.0 Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online are the school office
- The Governing Board will take overall responsibility for the website and delegate editorial responsibility to the Executive Headteacher to ensure that content is accurate and appropriate, and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers.

The school website complies with the statutory DfE guidelines for publications:

- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website is the school address and telephone number. The school uses a general email contact address; home information or individual email identities will not be published.
- Photographs published on the web do not have full names attached.
- The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- The school expects teachers using school approved blogs or wikis to password protect them and run from the school website.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that identified pupils cannot be recognised, or their image misused.
- The school will consider using group photographs as well than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
- Written permission from parents will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil.
- Pupil image file names will not refer to the pupil by name.

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

- The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Staff sign the school's Staff Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for their long-term use.
- The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

8.0 Social networking and personal publishing

- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system for such communications.
- School staff will ensure that in private use:
- No reference should be made in social media to pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

9.0 Managing filtering

- If staff or pupils come across unsuitable online materials, the site must be reported to

the computing lead and Office Manager
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

10.0 Managing videoconferencing and webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised.

11.0 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The Senior Leadership Team, SLT, should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

12.0 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

13.0 Personal devices and mobile phones

- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Executive Headteacher.

Such authorised use is to be monitored and recorded.

- Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times. Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times. Children are required to hand their mobile phones to the school office. The mobiles phones will be turned off.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are permitted to be used in certain areas within the school site, e.g. the staff room but always away from children.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will use the office phone where contact with pupils' parents is required.
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods, unless permission has been granted by a member of the SLT in emergency circumstances.

- Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, a school mobile phone will be provided and used. In an emergency where a staff member needs to use their own device they will hide the number by inputting 141 prior to the contact number
- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil brings technological items to school the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents in accordance with the school policy.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupil should bring their mobile phone or personally-owned device into school without consent from the Executive Headteacher. Any device brought into school without permission will be confiscated.

14.0 Policy decisions

Authorising Internet Access

- All staff will read and sign the Staff, Governor and Visitor Acceptable Use Agreement before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- In EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials. In KS2 access to the internet must be supervised by an adult and no pupils are to access Ipads without dult supervision.
- Any person not directly employed by the school will be asked to sign the Staff, Governor and Visitor Acceptable Use Agreement before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Executive Headteacher.
- Complaints of a safeguarding or child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see school's complaints policy)
- Pupils and parents will be informed of the consequences for pupils misusing the internet.

Community use of the internet

- The school will liaise with local organisations to establish a common approach to e-safety, if necessary.

15.0 Pupil online safety curriculum

- This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum and taught specifically during internet safety week.

This covers a range of skills and behaviours appropriate to the age of the children, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To know how to narrow down or refine a search.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.

To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.

- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- The school will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every pupil will sign.
- All staff will model safe and responsible behaviour in their own use of technology during lessons

16.0 Keeping Children Safe Online

The use of technology has become a significant component of many safeguarding issues such as child sexual exploitation and radicalisation and technology often provides the platform that facilitates harm. We recognise that children are at risk of abuse online as well as face to face and in many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, child-on-child abuse can take the form of abusive, harassing, and misogynistic messages, the consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery) and the sharing of abusive images and pornography.

We will seek to keep children safe by:

- delivering online safety through our computing and PSHE curriculums
- providing clear and specific directions to staff and volunteers on how to behave online through our staff code of conduct
- supporting and encouraging our pupils to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online

- keeping parents and carers up-to-date with any new worrying online concerns such as viral challenges and inappropriate apps.
- developing an online safety agreement for use with our pupils and their parents/carers
- 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/young person
- ensuring personal information about our pupils and their parents and carers is held securely and shared only as appropriate
- ensuring that images of children are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- 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.
- ensuring all staff are aware of the potential risks when pupils are online and how to record and respond to concerns appropriately.

Whilst regulation and technical solutions are very important, at Forest Edge Federation we also educate our pupils to take a responsible approach. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. 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; for example, pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If staff and/or pupils are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. All staff receive annual e-safety training to ensure they are aware of e-safety concerns and how these can be addressed with our pupils. In all cases, if staff are unsure, they should always speak to the Designated Safeguarding Lead (or deputy). These concerns will then be logged on My Concern and the appropriate action taken.

17.0 Responding to Online Abuse

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 on dealing with all forms of abuse, including bullying/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.

18.0 Links to other policies

- Safeguarding Policy
- Acceptable Use Agreement
- Code of Conduct Policy
- Whistleblowing Policy
- Behaviour Policy

- Computing Policy
- PSHE Policy