The Federation of Boskenwyn & Germoe Schools

and Nysgerrig Kindergarten

Acceptable Use and Online Safety policy (includes filtering and monitoring statement)

Information and Communications Technology (ICT) is seen in the 21st Century as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

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

o Websites
o Virtual Learning Environments
o E-mail and Instant Messaging
o Chat Rooms and Social Networking
o Blogs and Wikis o Podcasting
o Video Broadcasting
o Music Downloading
o Gaming
o AI technology
o Mobile/ Smart phones with text, video and/ or web functionality
o Other mobile devices with web functionality and wearable technology e.g smart watches

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At the Federation of Boskenwyn and Germoe Schools and Nysgerrig kindergarten, we understand the responsibility to educate our pupils regarding Online Safety issues; teaching them the appropriate behaviours, critical thinking skills and digital resilience to enable them to remain both safe and legal when using the internet and related technologies, both in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors, parents/carers and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils, parents, staff and visitors but brought onto school premises (such as laptops, mobile phones, camera phones, smart watches/fitness trackers and portable media players, etc).

The aims of this policy are to:

• Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
• Identify and support groups of pupils that are potentially at greater risk of harm online than others
• Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
• Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
• Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies.
• Safeguard and protect the children and staff of the federation of Boskenwyn and Germoe Schools and Nysgerrig kindergarten using the internet, social media or mobile devices
• Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own professional standards and practice to role model positive behaviour online.
• Set clear expectations of behaviour and/or Codes of Practice relevant to responsible use of the internet for educational, personal or recreational use.
• Have clear structures to deal with online abuse such as online bullying, which are cross referenced with other school policies.
• Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
• Ensure the curriculum teaches children how to make the correct choices online and know whom to speak to enable them to keep safe.
• Minimise the risk of misplaced or malicious allegations made against adults who work with children.
• To protect children from maltreatment, whether that is within or outside the home, including online (KCSiE 2026).

The 4 key categories of risk:

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

Content
• content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories

Contact
• contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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
• conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying

Commerce
• Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. (Ref Inspecting e safety Ofsted 2014, KCSiE 2026)

Legislation and guidance

The policy is based on the DfE statutory guidance 'Keeping Children Safe in Education' 2026 and its advice for schools on:

o Teaching online safety in schools
o Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
o Searching, screening and confiscation

It reflects existing legislation, including but not limited to 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 programmes of study.

Our schools will act in accordance with the Prevent Duty, which explains the schools' duties under the Counter-Terrorism and Security Act 2015 with respect to protecting people from the risk of radicalisation and extremism.

The policy will reflect DfE Filtering and Monitoring Standards (2022).

It takes into account the Early Years Foundation Stage (EYFS) Statutory Framework - (www.gov.uk) (updated September) and its advice on screen time.

This policy applies to all members of the federation of Boskenwyn and Germoe Schools and Nysgerrig Kindergarten community, including staff, students, pupils, volunteers, parents, carers and visitors.

The federation of Boskenwyn and Germoe Schools and Nysgerrig kindergarten will deal with such incidents within this policy and the Anti-bullying policy and will, where known, inform parents/ carers of incidents of inappropriate online safety behaviour that takes place out of school.

Review and Monitoring

The importance of online safety is referenced within other school policies: Safeguarding and Child Protection policy, Behaviour policy, Anti-bullying policy and RSHE policy.

• The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
• The Online Safety policy has been written by the school Designated Safeguarding Leader (DSL) and is current and appropriate for its intended audience and purpose.

• There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safety policy will be discussed in detail with all members of teaching staff.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA), KCSiE 2026, DfE Filtering and Monitoring Standards 2022.

Breaches

A breach or suspected breach of policy, by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected of ICT must be immediately reported to the Headteacher, DSL or Online Safety Leader, Lewis Hemsley. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher, DSL or Online Safety leader.

Equal Opportunities for Pupils with Additional Needs

The school endeavours to create a consistent message with parents and carers of all pupils and this in turn should aid establishment and future development of the school's online safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children and young people.

Online Safety Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The DSL in this school is Paula Blackburn who has been designated this role as a member of the senior leadership team. The Online Safety Leader is Lewis Hemsley. All members of the school community have been made aware of who holds these posts. It is the role of the DSL, supported by the DDSLs, to keep abreast of current issues and guidance through organisations such Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:
o Safeguarding and Child Protection
o Behaviour Policy
o Anti-bullying policy
o RSHE policy

Key Responsibilities

Headteacher/ ICT Lead

• The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
• Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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
• Along with the DSL and Online Safety lead, conducting a full security check and monitoring the school's ICT systems on a weekly basis
• Checking the systems in place block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
• Ensuring that any online safety incidents are logged (see Appendix 4) 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

Designated Safeguarding Lead and deputy safeguarding leads

Details of the school's designated safeguarding lead (DSL) and DDSLs are set out in our Safeguarding and Child Protection and policy, as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:
• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
• Promotes an awareness and commitment to online safeguarding throughout the school community
• Takes the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks without unreasonably impacting teaching and learning.
• Supports the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
• Works with the governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

Governors / Online safety governor

Key Responsibilities
• Works with the IT provider to make sure the appropriate systems and processes are in place with regards to filtering and monitoring (see Appendix 4 and Appendix 6).
• Liaises with the school Computing Lead to make sure appropriate systems and processes are in place to address any online safety issues or incidents
• Managing all online safety issues and incidents in line with the school's Safeguarding and Child Protection policy
• Ensuring that any pupil online safety incidents /cyber-bullying are logged on My Concern and dealt with appropriately in line with this policy and dealt with appropriately in line with the school behaviour policy
• Providing regular reports on online safety in school to the governors as part of the safeguarding report
• Undertaking annual risk assessments that consider and reflect the risks children face
• Are regularly updated in Online Safety issues and legislation, and be aware of the potential for safeguarding issues to arise from:
o sharing of personal data

o access to illegal / inappropriate materials
o inappropriate on-line contact with adults / strangers
o cyber-bullying and use of social media.
o potential or actual incidents of grooming

All governors will:
• Ensure they have read and understand this policy.
• Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1)
• Ensure that online safety is a running and interrelated theme within the whole-school approach to safeguarding and related policies and/or procedures
• Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
• To ensure that staff have online safety training and are provided with updates (via emails, briefing and annual training) so they know their expectations, roles and responsibilities to keep the children and staff safe.
• To ensure children are taught how to keep themselves safe, including keeping safe online.
• To ensure appropriate filtering and monitoring systems are in place and discuss with IT staff and ICT4 what needs to be done to support the school in meeting those standards, which include:
- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.
• To approve the Online Safety policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

Computing Curriculum Leader
• The Computing Curriculum Leader will oversee the continuous delivery of the online safety element of the computing curriculum and ensure it embedded across the curriculum
• To liaise with the DSL and Online Safety Lead regularly.
• To liaise with ICT4 with relation to the school's IT system, networks and filtering and monitoring.

ICT4 technician
• To report any online safety related issues that arise, to the DSL, Headteacher/DDSL or Online Safety leader/DDSL
• To ensure that users may only access the school's networks through an authorised and properly enforced password protection
• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date
• To ensure the security of the school IT system.
• To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
• The school's procedure on web filtering is applied and updated on a regular basis.
• To keep up to date with the school's Online Safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
• To maintain logs of incidents linked to alerts and take appropriate action after speaking with the DSL/DDSLs.

• To ensure that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, DSL or Online Safety leader, for investigation.
• To work alongside the school to ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
• To keep up-to-date documentation of the school's online security and technical procedures.

Teachers
• Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
• To plan and teach focused online safety lessons at least termly.
• To embed online safety issues in all aspects of the curriculum and other school activities.
• To ensure all pupils are aware of their Acceptable Use responsibilities
• To supervise and guide pupils carefully when engaged in learning activities involving online technology, including extra-curricular and extended school activities if relevant.
• Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
• Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by logging incidents onto My Concern and communicating with parents.
• Following the correct procedures by contacting the DSL who will liaise with ICT4 if they need to bypass the filtering and monitoring systems for a short period for educational purposes to resolve overblocking/underblocking

All staff and volunteers
• To read, understand, implement and help promote the school's Online Safety policies and guidance.
• Online Safety policy to be part of school induction pack for new staff.
• To read understand, sign and adhere to the school Acceptable Use Agreement and Policy.
• To be aware of online safety issues related to the use of mobile phones, cameras, wearable or hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
• To report any suspected misuse or problem to the online safety lead/DSL
• To maintain an awareness of current online safety issues and guidance e.g. through CPD
• To model safe, responsible and professional behaviours in their own use of technology
• To ensure that any digital communications with parents and pupils should be on a professional level and only through school-based systems. For exceptions, see Mobile Phone policy
• Deliberate access to inappropriate materials by any user will lead to the incident being logged by the DSL, depending on the
• Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 1), and ensuring that pupils follow the school's terms on acceptable use
• Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
• Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.
• Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
• Working with the DSL to ensure 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

• Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
• All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the DSL/Online Safety Lead.
Deliberate access to inappropriate materials by any user will lead to the incident being logged by the DSL, depending on the seriousness of the offence, investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Pupils
• Understand and adhere to the rules around acceptable use and online safety.
• To understand the importance of reporting misuse or access to inappropriate materials.
• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
• To understand the importance of adopting good online safety practice when using digital technologies out of school.
• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home.

Parents/carers
• To support the school in promoting online safety and endorse the Pupil Acceptable Use Agreement which includes the pupils' use of the internet
• Should know and understand what the term 'appropriate use' is.
• To give permission for school's use of photograph and video images.
• To consult with the school if they have any concerns about their children's use of technology.
Parents/carers can access further information on keeping their children safe online from the school website or by accessing advice from the following organisations and websites:
• What are the issues? – UK Safer Internet Centre
• Hot topics – Childnet
• Parent resource sheet – Childnet

Visitors and members of the community
• Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

External groups
• Any external individual / organisation will be made aware of this policy, when relevant, and expected to read and follow it.

The Online Safety Curriculum:

There is a clear, progressive online safety education programme as part of the Computing curriculum and RSHE learning from EYFS to Year 6.
All schools have to teach:
Relationships education and health education in primary schools
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

• Identify a range of ways to report concerns about content and contact
By the end of primary school, pupils will know:
• That people sometimes behave differently online, including by pretending to be someone they are not
• That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
• The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
• How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
• How information and data is shared and used online
• What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
• How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
• 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 or carer, teacher or trusted staff member, or an organisation such as ChildLine.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

An essential part of the online learning provision will be ensuring our children have clear reporting routes in place, so they can raise any concerns whilst online. The following links are available on our website:
Staying Safe Weblinks
• 'Kidsmart' - Resources for staying safe online
• Child Exploitation and Online Protection (CEOP)
• Childline Bullying Information and Advice
• SWGfL Helpful information leaflets for parents
• Internet Matters - Helping parents keep their children safe online
• NSPCC Bullying & Cyberbullying
• NSPCC Share Aware
• Think You Know How - CEOP

In addition, the school website has the Report Harmful Content button (IWF) available for children to access and use. This means that children will be easily able to locate support and information each week should they need it. They will be able to contact their teacher or support staff with an online safety concern or use this information to seek help from alternative safe sources if their adults are not available

Parental Communication about Online Safety:

The school will raise parents/carers' awareness of internet safety in newsletters or other communications home, and in information via our website or Seesaw.

The policy will be communicated to staff, pupils, governors and the community in the following ways:
• Policy to be posted on the school website and emailed to staff
• Weekly newsletters with signposts for parents
• The policy will be discussed agreed in full governing body meetings

Handling complaints

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

• Staff and pupils are given information about consequences for unacceptable use and possible sanctions. Sanctions available include:

o Discussion with class teacher, Online Safety Leader, DSL, Headteacher.

o Informing parents or carers.

o Removal of internet or computer access within school for a period.

o Referral to LA / Police

o Accessing extremist material could result in a referral to 'Channel'.

• Any complaint about staff misuse is referred to the Headteacher.

• If the complaint is regarding the Headteacher, the Chair of Governors should be contacted.

• Complaints of cyber-bullying are dealt with in accordance with our Anti-bullying policy. Complaints related to safeguarding are dealt with in accordance with school and LA child protection procedures as a maintained school.

Password guidance

• This school makes it clear that staff and pupils must always keep their personal password private, must not share it with others and must not leave it where others can find it.

• All staff and children have their own unique username and private passwords to access school systems.

• We require staff to use STRONG passwords to ensure school information/data is kept safe using a 'complex' password. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).

Social Media

• The school's system for social networking will be maintained in adherence with this policy. The school networking sites are updated and moderated by members of school staff.

School staff will ensure that in private use:

• They do not accept or request pupils as 'friends' on social networking sites or exchange personal email addresses or mobile phone numbers with students.

• They do not publish defamatory and /or false materials about the federation of Boskenwyn and Germoe Schools and Nysgerrig Kindergarten

• No reference should be made in personal social media to pupils in which they could be identified

• 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 local authority.

• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

• Staff agree not to publish content that may be considered threatening, hurtful or defamatory to others and to consider the appropriateness of sharing specific and detailed private thoughts, concerns, images or messages on any social media services. Staff must have an awareness at all times of the school's digital footprint.

Cyber-bullying

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.

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. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE and RSHE education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also signposts information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti bullying policy and 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 DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Our schools recognise that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Generative AI- The school will take account of guidance published by the DFE Generative AI: product safety expectations to support us to use generative artificial intelligence safely. The school recognises that Artificial Intelligence technologies may create safeguarding risks through:
- deepfake imagery;
- AI-generated sexual content;
- impersonation;
- misinformation;
- image manipulation;
- exploitation through AI chatbots;
- technology-facilitated abuse.

Concerns relating to AI will be managed through Concerns relating to AI will be managed through existing safeguarding procedures. The school will treat any use of AI to bully pupils in line with our Anti-bullying and Behaviour policies.

As a precaution, the AI overview has been removed from search engines by our provider of filtering and monitoring services, ICT4.

Online Hate

The school will take all reasonable precautions to ensure that
• Online hate content, directed towards or posted by, specific members of the community will not be tolerated at our schools and will be responded to in line with existing policies, including anti-bullying, safeguarding, the Equality Duty and behaviour.
• All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
• The police will be contacted if a criminal offence is suspected.
• If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the LA Safeguarding Team and Devon and Cornwall Police.

Online Radicalisation and Extremism

Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

N.B. Counter-Terrorism and Security Act 2015 (and the Prevent Duty guidance, updated 2023): The Act places a Prevent duty on specified schools to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent Duty. Schools must have regard to statutory guidance issued under section 29 of the CTSA 2015 ("the Prevent guidance"). The education and childcare specified authorities in Schedule 6 to the Act are as follows:

Schools/settings subject to the Prevent Duty will be expected to demonstrate activity in the following areas:
• Assessing the risk of children being drawn into terrorism
• Demonstrate that they are protecting children and young people from being drawn into terrorism by having robust safeguarding policies.
• Ensure that their safeguarding arrangements take into account the policies and procedures of the Local Safeguarding Children Board.
• Make sure that staff have training that gives them the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism
• Expected to ensure children are safe from terrorist and extremist material when accessing the internet in school
• Learners and staff are safe from terrorist and extremist material when accessing the internet on site.
• If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding policy.
• If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Safeguarding and Whistleblowing and policies.

Equipment and Digital Content

Staff and Visitors Personal mobile phones and mobile devices

• Mobile phones brought into school are entirely at the staff member, parents' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
• Parents/carers and visitors (including volunteers and contractors) must not use their mobile phones and personal devices on site, in accordance with our acceptable use and mobile phone policy.
• Staff should use their mobile phones in compliance with the mobile phone policy
• Staff are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
• It is the responsibility of the adult to ensure that there is no illegal or inappropriate content stored on their device when brought onto the school grounds.
• Personal mobile phones should never be used to contact children, young people or their families, apart from in exceptional circumstances, such as on a school trip.
• Personal devices should not be used to take videos or photographs of the children. However, in exceptional circumstances, such as offsite activities, trips or visits, permission may be granted by the Headteacher, provided there is an agreed timescale for transfer and deletion of the image from the staff member's device. See mobile phone policy.

Pupils' use of personal devices

The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone e.g. when moving between parents. In this case, the phone will be handed in to the class teacher and locked away during the school day. Pupils must not use mobile phones or SMART devices when on the school premises. Mobile phones brought into school are entirely at the pupil's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
• Poses a risk to staff or pupils, and/or
• Is identified in the school rules as a banned item for which a search can be carried out, and/or
• Is evidence in relation to an offence
Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
• Make an assessment of how urgent the search is, and consider the risk to other pupils and staff and then seek advice from the Head teacher/DSL.
• Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
• Seek the pupil's co-operation.
If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
• Not view the image
• Confiscate the device and report the incident to the DSL or Head teacher immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
The Head teacher or DSL may examine, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so, such as:

• Cause harm, and/or
• Undermine the safe environment of the school or disrupt teaching, and/or
• Commit an offence

If it is believed inappropriate material is on a pupil device, it is up to the DSL and/or Head teacher to decide on a suitable response. If it is believed that there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

• They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
• The pupil and/or the parent/carer refuses to delete the material themselves

Any searching of pupils will be carried out in line with:

• The DfE's latest guidance on searching, screening and confiscation
• UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

• Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
• Making sure the device locks if left inactive for a period of time
• Not sharing the device among family or friends
• Allowing the network anti-virus and anti-spyware software to run
• Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 1.

If staff have any concerns over the security of their device, they must seek advice from the computing or technical staff.

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 our policies on Behaviour, Antibullying and Acceptable Use Agreement (Appendix 1). 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 /staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive safeguarding training, as part of their induction, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings). By way of this training, all staff will be made aware that:

• Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
• Children can abuse their peers online through:
o Abusive, threatening, harassing and misogynistic messages
o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
o Sharing of abusive images and pornography, to those who don't want to receive such content
• Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

• Develop better awareness to assist in spotting the signs and symptoms of online abuse
• Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
• Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs 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.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

Incident Reporting

Online Safety Incident Log and Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the DSL or Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher and/or the DSL

Incident Reporting Procedure:

• If an incident is reported to a member of staff it needs to be reported to the DSL or Online Safety Leader and logged
• The child/children and/or all parties involved should be spoken with (if appropriate) to gain a full and fair understanding of the incident.
• Staff will record concerns on My Concern and also discuss concerns directly with the Headteacher, DSL or Online Safety Leader
• A member of staff will make contact with the parents/carers if appropriate.
• Outside agencies will be involved when appropriate e.g. the LA, police, CEOP and LA Online Safety Officer.
• The incident is then discussed and next steps agreed to put in any consequences if appropriate and /or to provide support for children involved to ensure they understand Online Safety regulations and reiterate Online Safety rules set out by the school following the National Guideline.
• Historic incident logs are all locked in a secure cupboard.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL and Online Safety Lead/DDSL. At every review, the policy will be shared with the governing board.

Links with other policies

This Online Safety policy is linked to our:
- Safeguarding and Child Protection policy
- Behaviour policy
- Staff disciplinary procedures
- Data Protection policy and privacy notices
- Complaints procedure
- Anti-Bullying policy

This policy was reviewed in September 2026. It will be reviewed annually.

Paula Blackburn, Executive Headteacher

Lucy Yeomans, Chair of governors

Appendix 1

Acceptable Use Agreement: Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. The Online Safety 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 to say they have read this policy and adhere at all times to its contents, as well as the key points restated below. Any concerns or clarification should be discussed with Paula Blackburn or Lewis Hemsley

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body.
- 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 (unless in emergency on trips and visits), personal e-mail address, personal Twitter account, or any other social media link, to pupils and will not request or add pupils as 'friends' on social media.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick.
- 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 in line with school policy and with written consent of the parent, carer or staff member.
• Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
• I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community.
• 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/Online safety Lead.
• I will respect copyright and intellectual property rights.
• I will ensure that my online activity, both in school and outside of 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 policy 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 the classroom between the hours of 8.30am and 3.30pm (except in exceptional circumstances stated in the mobile phone policy)
• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

User Signature

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 ……..(printed)

Job title ……

This agreement can be signed at the school office upon arrival to the school.

Filtering and Monitoring Statement

The federation of Boskenwyn and Germoe Schools and Nysgerrig Kindergarten:

• Has the educational filtered secure broadband connectivity through ICT4.
• Uses the Senso alerting filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
• The school use Senso Alerting via ICT4 as its monitoring systems
• Uses a DfE, LA approved system, Microsoft SharePoint using encrypted password protected links. Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
• Only unblocks other external social networking sites for specific purposes such as Internet Linked lesson lessons.
• Has blocked pupil access to music download or shopping sites, except those approved for educational purposes at a regional or national level.
• Uses security time-outs on internet access where practicable and useful.
• Works in partnership with ICT4 and Senso alerting to ensure any concerns about the system are communicated so that systems remain robust and protect students.
• Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.

• Ensures all staff have signed an acceptable use agreement form and understands that they must report any concerns.
• Ensures pupils only publish within an appropriately secure environment the school's learning environment.
• Requires staff to preview websites before use and may direct students to subject and age appropriate web sites
• Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
• Informs all users that internet use is monitored.
• Informs staff and students that they must report any failure of the filtering systems directly to the teacher, DSL, online safety lead so they can be logged or escalated to the ICT4.
• Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse through staff meetings and teaching programmes.
• Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents.
• Immediately refers any material we suspect is illegal to the appropriate authorities - Police and the LA.