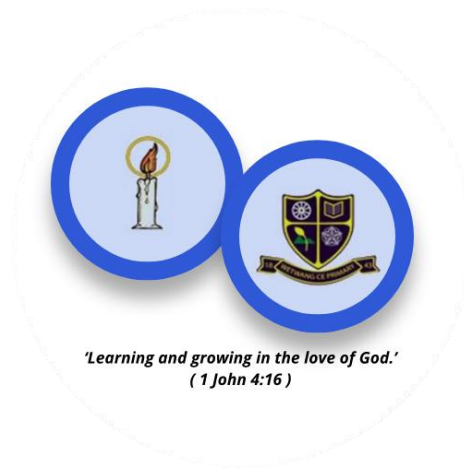




Sledmere and Wetwang Federation

E-SAFETY POLICY – January 2026

Adopted by Sledmere and Wetwang Federation Policy Review Group

Signed: Andrew McCormack

Position: Chair of Governors

To be reviewed by Governors January 2027

Vision

‘Learning and growing in the love of God’ (1 John 4:16)

Introduction

At Sledmere and Wetwang Federation we fully recognise, acknowledge and embrace the importance and benefits of a 'connected' world. The opportunities for learning created by providing access to such a world are limitless, and must therefore become part of day-to-day teaching and learning in school. Being part of the internet community, as well as providing the aforementioned opportunities, also opens up the possibilities of exposure to dangers which would otherwise not be present, for example: access to inappropriate materials, contact with potentially dangerous strangers, 'cyber' bullying and identity theft. It must therefore be the role of the school to ensure that such risks are minimized, and, more importantly, that children are provided with the knowledge, skills and attitude necessary to become positive, safe and healthy on-line citizens.

Responsibilities of the school community

We believe that e-safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

- Develop and promote an e-safety culture within the school community
- Support the e-safety coordinator in their work
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to e-safety effectively
- Receive and regularly review e-safety incident logs and be aware of the procedure to be followed should an e-safety incident occur in school
- Take ultimate responsibility for the e-safety of the school community Responsibilities of the e-safety co-ordinator
- Promote an awareness and commitment to e-safety throughout the school
- Be the first point of contact in school on all e-safety matters
- Create and maintain e-safety policies and procedures
- Develop an understanding of current e-safety issues, guidance and appropriate legislation
- Ensure all members of staff receive an appropriate level of training in e-safety issues
- Ensure that e-safety education is embedded across the curriculum
- Ensure that e-safety is promoted to parents and carers
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate
- Monitor and report on e-safety issues to the e-safety group and SLT as appropriate
- Ensure an e-safety incident log is kept up-to-date Responsibilities of Teachers and Support Staff
- Read, understand and help promote the school's e-safety policies and guidance
- Read, understand and adhere to the Acceptable Use Policy (AUP) and Social Media Policy
- Develop and maintain an awareness of current e-safety issues and guidance
- Model safe and responsible behaviours in your own use of technology
- Embed e-safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Be aware of what to do if an e-safety incident occurs
- Maintain a professional level of conduct in their personal use of technology at all times

Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's e-safety policies and guidance
- Read, understand and adhere to the school staff AUP
- Support the school in providing a safe technical infrastructure to support learning and teaching
- Take responsibility for the security of the school computing system
- Report any e-safety-related issues that come to your attention to the e-safety coordinator
- Develop and maintain an awareness of current e-safety issues, legislation and guidance relevant to your work
- Liaise with the local authority and others on technical issues
- Maintain a professional level of conduct in their personal use of technology at all times

Responsibilities of Pupils

- Read, understand and adhere to the school pupil AUP
- Help and support the school in creating e-safety policies and practices; and adhere to any policies and practices the school creates
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home
- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to
- Discuss e-safety issues with family and friends in an open and honest way
- We will develop and support peer-led online safety strategies. Pupils are encouraged to take responsibility for 'each other's safe and responsible use of technology' by acting as digital mentors who can help peers identify risks and feel confident in using the school's reporting channels

Responsibilities of Parents and Carers

- Help and support your school in promoting e-safety
- Read, understand and promote the school pupil AUP with your children
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss e-safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Model safe and responsible behaviours in your own use of technology
- Consult with the school if you have any concerns about your children's use of technology

Responsibilities of Governing Board

- Read, understand, contribute to and help promote the school's e-safety policies and guidance
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupil
- Develop an overview of how the school computing infrastructure provides safe access to the Internet

- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- Support the work of the e-safety co-ordinator in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safety activities
- Ensure appropriate funding and resources are available for the school to implement their e-safety strategy

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide a series of specific e-safety-related lessons in every year group/specific year groups as part of the computing curriculum / PSHE curriculum / other lessons
- We will celebrate and promote e-safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year
- We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials
- We will remind pupils about their responsibilities through an end-user AUP which every pupil will sign/displayed throughout the school/displayed when a pupil logs on
- Staff will model safe and responsible behaviour in their own use of technology during lessons
- The Federation recognises that effective online safety is based on the '4 Cs' framework: Content, Contact, Conduct, and Commerce. While protecting children from inappropriate materials and strangers, we also commit to educating pupils on the risks of online Commerce, including inappropriate advertising, online gambling, and financial scams, extending beyond our existing protections for identity theft

Artificial Intelligence

In line with the Federation's Artificial Intelligence Policy, online safety education will encompass the unique risks of emerging technologies. We will 'promote critical evaluation of information provided by AI' to help pupils identify deepfakes, AI-generated misinformation, and biased content. All AI integration will maintain a focus on 'safeguarding data privacy in compliance with GDPR' as an interrelated safeguarding theme

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this, we will:

- hold an annual parent meeting on e-safety / include e-safety as part of an annual parent meeting
- include useful links and advice on e-safety regularly in newsletters / on our school website
- include a section on e-safety in the school handbook
- To ensure the entire school community is protected, online safety information and reporting routes will be provided in a variety of accessible formats. This includes providing materials in alternative languages for families with English as an additional language (EAL) and ensuring resources are adapted for pupils with SEND to ensure 'equitable access to education' and safety

Managing Computing Systems and Access

The school will be responsible for ensuring that access to the computing systems is as safe and secure as reasonably possible

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access
- Servers, workstations and other hardware and software will be kept updated as appropriate
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school computing systems, and that such activity will be monitored and checked
- Members of staff will access the Internet using an individual log-on. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times
- Any administrator or master passwords for school computing systems should be kept secure and available to at least two members of staff, e.g. Headteacher/ Business Manager and member of technical support
- The wireless network in school is encrypted to reduce the risk of unauthorised access
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur
- The school will regularly audit computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

Filtering Internet Access

- The school uses a filtered Internet service. The filtering is provided through Smoothwall.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-safety coordinator
- If users discover a website with potentially illegal content, this should be reported immediately to the e-safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, CEOP or IWF
- The school reviews the filtering and other security systems to ensure they meet the needs of all users monthly.

Learning technologies in school

Aspect	Pupils	Staff
Personal mobile phones brought into school	N	Y – streaming music in Collective Worship
Mobile phones used in lessons	N	Not if avoidable
Mobile phones used outside of lessons	N	Not if avoidable
Taking photographs or videos on personal equipment	N	Y - Photos to be downloaded to school laptop ASAP to increase security.
Taking photographs or videos on school devices	Y	Y
Use of hand-held devices such as	N	Y

PDA's, MP3 players or personal gaming consoles		
Use of personal email addresses in school	N	Y
Use of online chat rooms	N	N
Use of instant messaging services	N	N
Use of blogs, wikis, podcasts or social networking sites	Y – controlled by filtering	Y – controlled by filtering
Use of video conferencing / online video meetings	Supervised	Y

Using email

- Pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked
- Staff should use their school e-mail address for correspondence relating to school
- Classes may be allocated an individual e-mail account for use by pupils within that class, under supervision of the class teacher
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments
- Pupils are not permitted to access personal e-mail accounts during school
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately

Using images, video and sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home
- Digital images, video and sound will be created using equipment provided by the school, or equipment owned by staff who have signed the agreement in the staff AUP, that images of children will not be kept on personally owned computer equipment
- Staff and pupils will follow the school policy on creating, using and storing digital resources
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved • If pupils are involved, relevant parental permission will also be sought before resources are published online

Using blogs, wikis, podcasts, social network and other ways for pupils to publish content online

We may use blogs/wikis/podcasts/social networking/other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within the areas the school has provided for such material. These will include: the school website, school blogs, hosted by WordPress, Twitter and YouTube

- Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school

Using video conferencing and other online video meetings

We occasionally use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner

- All video conferencing activity will be supervised by a suitable member of staff
- Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff
- Video conferencing equipment will be switched off and secured when not in use / online meeting rooms will be closed and logged off when not in use
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms
- Video conferencing should not take place off school premises without the permission of the Headteacher
- Parental permission will be sought before taking part in video conferences
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school

Using mobile phones

- Pupils' personal mobile phones are not allowed in school
- Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up such that only those features required for the activity will be enabled
- Use of staff mobile phones for school purposes will be refunded if necessary. Staff would prefer to carry and use their own mobile phones on school visits, rather than a 'school mobile'. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parents

Protecting Personal Data

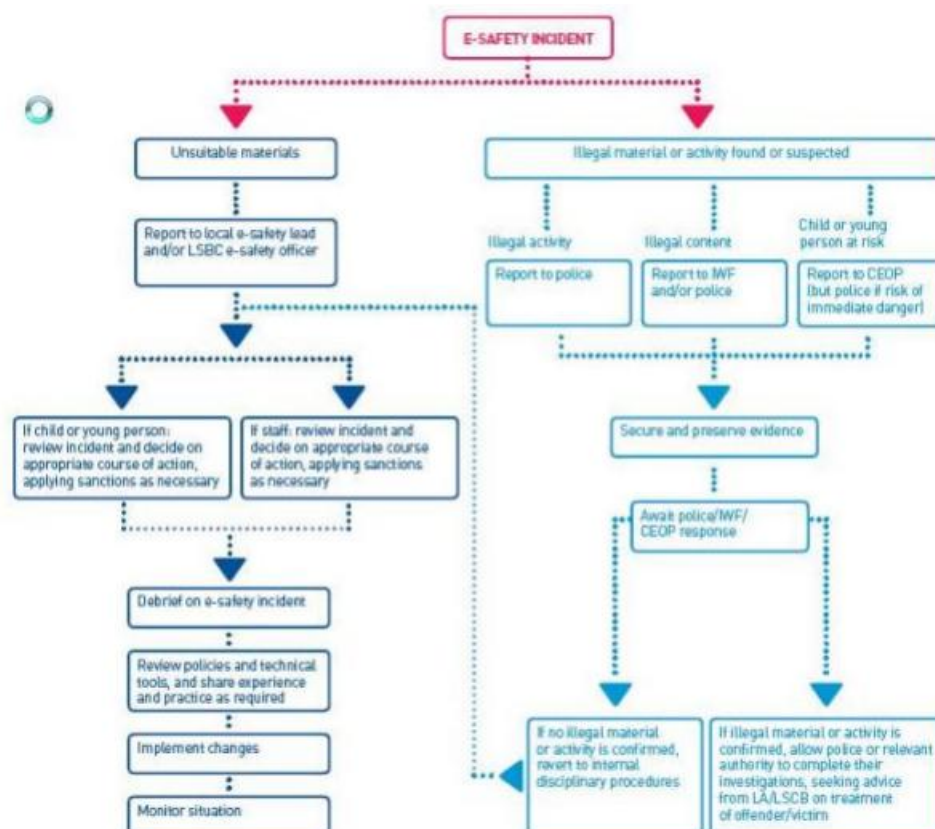
We will ensure personal data is recorded, processed, transferred and made available according to GDPR 2018

- Staff will ensure they properly log-off from a computer terminal after accessing personal data
- Staff will not remove personal or sensitive data from the school premises without permission of the Headteacher. Any data which is impractical to ensure is kept in school (eg Reports) will be kept secure, by use of school laptops which are password protected. All files which contain personal data will be individually password protected School Website and other online content published by the school
- The school website will not include the personal details, including individual e-mail addresses of staff or full names of pupils
- A generic contact e-mail address will be used for all enquiries received through the school website
- All content included on the school website will be approved by the head teacher before publication
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified

- Staff and pupils should not post school-related content on any external website without seeking permission first

Dealing with safety incidents

The school maintains clearly described procedures for responding to a variety of modern online harms. This includes specific protocols for managing incidents involving consensual and non-consensual nude and semi-nude image sharing, exposure to 'fake news', and online grooming. We utilise national reporting mechanisms, such as the Internet Watch Foundation (IWF) and CEOP, to escalate these concerns appropriately



The Federation is committed to a whole-school culture that empowers pupils to report issues without fear. We explicitly challenge 'victim-blaming' language and attitudes, recognising that 'children are never responsible for the harm which they may experience' online, regardless of their actions. Staff will provide non-judgemental support to all victims of online harms