

Skirlaugh CE Primary School
'a caring Christian learning community where everyone is valued'



Online Safety Policy

Approved by Governors

Summer 2024

Last Renewal Date

Spring 2026

Next Renewal Date

Spring 2027

Skirlaugh CE Primary School
'a caring Christian learning community where everyone is valued'

Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Skirlaugh CE Primary School involving staff, pupils and parents/carers, building on the East Riding Yorkshire Council online safety guidance, with specialist advice and input as required.
- This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
 - Teaching online safety in schools
 - Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
 - Relationships and sex education
 - Searching, screening and confiscation
- It also refers to the DfE's guidance on protecting children from radicalisation.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
- The policy also takes into account the National Curriculum computing programmes of study.
- The purpose of Skirlaugh CE Primary School's online safety policy is to:
 - Safeguard and protect all members of Skirlaugh CE Primary School's community online.
 - Identify approaches to educate and raise awareness of online safety throughout the community.
 - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - Establish clear mechanisms to identify, intervene and escalate an incident or online safety concern, where appropriate
- Skirlaugh CE Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
 - **Content:** being exposed to illegal, inappropriate or harmful material
 - **Contact:** being subjected to harmful online interaction with other users
 - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm
 - **Commerce:** risks such as online gambling, inappropriate advertising or financial scams

2. Policy Scope

- Skirlaugh CE Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Skirlaugh CE Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Skirlaugh CE Primary School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.1 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP) (Appendix A and B) and/or the Code of Conduct
 - Behaviour policy
 - Strategic Child Protection & Safeguarding policy
 - Confidentiality policy
 - Curriculum documents, such as: Computing, Personal Social and Health Education (PSHE) and Sex and Relationships Education (SRE)
 - GDPR

3. Monitoring and Review

- Skirlaugh CE Primary School will review this policy at least annually
 - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body any online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The school has appointed Miss N Davis as Designated Online Safety Coordinator.
- The governor with specific responsibility for online safety is Reverend David Messer.
- Skirlaugh CE Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Leadership and Management Team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of Conduct and/or an AUP which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.

- Work with LA technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Carefully consider and assess any use of generative AI by staff and pupils, evaluating the benefits and risks of use. The use of AI will be in line with the appropriate DfE guidance and policy for AI.
- Support the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL), in conjunction with the Online Safety Coordinator will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Ensure that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour and anti bullying policies
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

4.3 It is the responsibility of all members of staff to:

- Ensure they fully understand this policy and contribute to its development/review
- Read and adhere to the online safety policy and AUPs.
- Explain AUPs to the children in their care and ensure these are upheld at all times.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever relevant, and whenever technology is being used.
- Understand that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or

expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. Teach children the importance of this so they are aware and can use it safely.

- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care, maintaining the attitude that 'it could happen here'.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Put 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
- Implement appropriate security measures (*including change of passwords and encryption*) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.

- Contribute to the development of the school online safety policies.
- Use school systems and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access and reminding pupils of these before using any technology or accessing the internet.
 - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology by pupils.
 - Implementing appropriate peer education approaches.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
 - Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.1.1 Vulnerable Pupils

- Skirlaugh CE Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Skirlaugh CE Primary School will ensure that differentiated and ability-appropriate online safety education, access and support is provided to vulnerable pupils. Skirlaugh CE Primary School will seek input from specialist staff as appropriate, including the SENDCO and Computing lead.

5.2 Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
 - This will cover the potential risks posed to pupils (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and carers

- Skirlaugh CE Primary School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
 - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, and sports days.
 - Drawing their attention to the school online safety policy and expectations in newsletters, letters, school prospectus and website.
 - Requesting that they read online safety information as part of joining our school, for example, Induction pack.
 - Requiring them to read the school AUP and discuss its implications with their children.

6. Reducing Online Risks

- Skirlaugh CE Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
 - Regularly review the methods used to identify, assess and minimise online risks.
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
 - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
 - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Skirlaugh CE Primary School uses a wide range of technology. This includes access to:
 - Computers, laptops and ipads
 - Internet which may include search engines and educational websites
 - Email
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place. For example all devices connected to the internet do so through a comprehensive filtering system, provided by East Riding Council IT support.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools such as SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledges the source of information.
- Supervision of pupils will be appropriate to their age and ability.
 - **Early Years Foundation Stage and Key Stage 1**
 - Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
 - **Key Stage 2**
 - Pupils will use age-appropriate search engines and online tools.
 - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Skirlaugh CE Primary School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate; this takes place weekly during the DSL safeguarding meeting.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through the Kcom Lightsteam service.
- The school uses Smoothwall Filtering which blocks inappropriate sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
 - The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with Smoothwall to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
 - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to a member of staff.
 - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
 - The breach will be recorded and escalated as appropriate.
 - Where appropriate, parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, East Riding Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
 - Physical monitoring through supervision in lessons
 - Monitoring of internet and web access (reviewing and investigating reported incidents via SmoothWall)
- The school has a clear procedure for responding to concerns identified via monitoring approaches: Usage alerts raised through SmoothWall are emailed to the Headteacher and Designated Safeguarding Lead (DSL). They will then liaise with staff members as to the possible reasons for the alert and record all findings. The DSL will then follow the safeguarding procedure as set out in the policy if required.
- Concerns raised through physical monitoring or by staff are reported directly to the DSL who will then follow the safeguarding procedure.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation.

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly.
 - Encryption for personal data sent over the internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on the school's network,
 - The appropriate use of user logins and passwords to access the school network.
 - Specific user logins and passwords will be enforced for all users.
 - All users are expected to log off or lock their screens/devices if systems are unattended.
 - Further information about technical environment safety and security can be found in the Acceptable Usage Policy (AUP).

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords yearly, or at the start of the academic year.
 - Always keep their password private; users must not share it with others, save it to their device or leave it where others can find it.
 - Not impersonate another user.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): the Image use statements, GDPR, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.

7.8 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.
 - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
 - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
 - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the Headteacher if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
 - All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

7.8.2 Pupils

- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the school.

7.9 Educational use of Videoconferencing and/or Webcams

- Skirlaugh CE Primary School recognise that videoconferencing and the use of webcams can be a challenging activity but brings a wide range of learning benefits.
 - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
 - Videoconferencing contact details will not be posted publicly.
 - School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.
 - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

7.9.1 Users

- Parent and carer consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

7.10 Management of Applications which Record Children's Progress

- The school uses Compass, Tapestry and B Squared to track pupils' progress.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation
- To safeguard data:
 - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content.
 - School devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft.
 - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
 - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images (in the case of Tapestry).

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Skirlaugh CE Primary School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chat rooms and instant messenger.
- All members of Skirlaugh CE Primary School's community are expected to engage in social media in a positive, safe and responsible manner, at all times.
 - All members of Skirlaugh CE Primary School's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school network does not allow pupil and staff access to social media whilst using school provided devices and systems on site at any time, with the exception of the school X (formerly Twitter) account.
 - The use of social media during school hours for personal use is not permitted.
 - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of Skirlaugh CE Primary School's community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - Setting the privacy levels of their personal sites as strictly as they can.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Skirlaugh CE Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
 - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
 - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the headteacher.
 - If on-going contact with pupils is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.

- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples could include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
 - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications and report concerns both within school and externally.

8.4 Official Use of Social Media

- Skirlough CE Primary School's official social media channel is our X(formerly Twitter) page.
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
 - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use school provided email addresses to register and manage school social media channels.
 - Official social media sites are suitably protected and linked to the school website.
 - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.

- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
 - Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
 - Any official social media activity involving pupils will be moderated by the school where possible.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
 - Sign the school's Acceptable Use Policy for staff.
 - Be professional at all times and aware that they are an ambassador for the school.
 - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
 - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
 - Ensure that they have appropriate written consent before posting images on the official social media channel.

Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

 - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
 - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils

9. Use of Personal Devices and Mobile Phones

- Skirlaugh CE Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
 - All members of Skirlaugh CE Primary School's community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
 - All members of Skirlaugh CE Primary School's community 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.

- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms or toilets.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of Skirlaugh CE Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child Protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child Protection, Data Security and Acceptable Use.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time, for example locked in a desk drawer.
 - Keep mobile phones and personal devices switched off or on 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled.
 - Not use personal devices during teaching periods, unless in emergency circumstances.
 - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
 - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
 - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
 - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Skirlaugh CE Primary School expects pupil's personal devices and mobile phones not to be brought onto site. Mobile phones brought onto site by pupils will be taken from the pupil and kept safe in school until the end of the school day, when they will be handed back.
- If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone.
 - Parents are advised to contact their child via the school office during school hours.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies.

- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

10. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
 - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Police.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with East Riding Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the East Riding Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- Skirlaugh CE Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- The school will follow the advice as set out in the non-statutory UKCCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) and [KSCB](#) guidance: “Responding to youth produced sexual imagery”.
- Skirlaugh CE Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with ‘Sexting’

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
 - Act in accordance with our Child protection and Safeguarding policies and the relevant East Riding Safeguarding Child Board’s procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store the device securely.
 - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Specialist Children’s Services and/or the Police, as appropriate.
 - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
 - Implement appropriate sanctions in accordance with the school’s Behaviour policy, but taking care not to further traumatised victims where possible.
 - Consider the deletion of images in accordance with the UKCCIS: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
 - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation

- Skirlaugh CE Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Skirlaugh CE Primary School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.

11.2.1 Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's Child protection and Safeguarding policies and the relevant East Riding Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform East Riding police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Make a referral to Specialist Children's Services (if required/ appropriate).
 - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
 - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or East Riding Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](#) (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from East Riding Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- Skirlaugh CE Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through East Riding Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
 - Act in accordance with the schools child protection and safeguarding policy and the relevant East Riding Safeguarding Child Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), East Riding Police Force or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
 - Ensure that the headteacher is informed.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Skirlaugh CE Primary School
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Skirlaugh CE Primary School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or East Riding Police.

11.6 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is 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 Child Protection and Allegations policies.

Appendix A: Acceptable Use Policies for Pupils

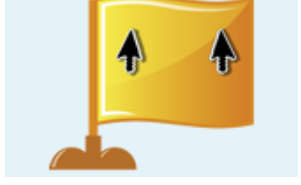


Skirlaugh CE Primary School

'a caring Christian learning community where everyone is valued'

Acceptable Use Rules

Early Years Foundation Stage and Key Stage 1

 Zip It Keep your personal stuff private and think about what you say and do online.	We must use the Internet safely to help us learn. We learn to keep our password just to ourselves or tell one trusted adult who can help us remember it. We don't ever tell anyone online our address or phone number.
 Block It Block people who send nasty messages and don't open unknown links and attachments.	We will only click on icons and links when we know they are safe. Only click on things your teacher has told you to. If you are not sure then ask an adult. We know that it is important to follow the rules.
 Flag It Flag up with someone you trust if anything upsets you or if anyone asks to meet you offline.	We know who to ask for help. If we see something we do not like we know that we should tell an adult. We know that some websites and social networks have age restrictions and we should not use them unless we are old enough. We know that our use of ICT can be checked and that our parent/carer will be contacted if a member of school staff is concerned about our safety.



Skirlaugh CE Primary School

'a caring Christian learning community where everyone is valued'

Acceptable Use Rules

Key Stage 2

 Zip It Keep your personal stuff private and think about what you say and do online.	I will be careful what information I put on the internet and who can see it. I will not give out personal information like email addresses, home or school addresses or phone numbers. I will not share my passwords and will remember to log off correctly when I have finished my work. I will not use digital technology to bully people or make threats. I will not send inappropriate emails. I agree not to send unsuitable pictures or films to anyone using the internet. I know that by sending images of this type I could be committing an offence. I will not use AI in school for my work unless it has been agreed with an adult.
 Block It Block people who send nasty messages and don't open unknown links and attachments.	I agree not to access sites that are not suitable for my age. I will not access game sites or social network sites during school times. I will be careful who I chat to and make friends with on game sites or Social Networking sites. I will not try to join a site if I am younger than its age limit. I agree not to contact, or arrange to meet people I do not know using the internet or other technology. I will not open emails or attachments from people I do not know before checking with a teacher or adult. I will not respond to upsetting messages and cyber-bullying.
 Flag It Flag up with someone you trust if anything upsets you or if anyone asks to meet you offline.	If I receive an upsetting message I will keep the message and show it to an adult. I will tell adults about anything I find (like an unsuitable website) that I am worried about or I think is unsuitable. I will tell an adult if we suspect that someone else is being bullied on the internet or accessing inappropriate material. I know that my use of ICT can be checked and that my parents/carers will be contacted if a member of school staff is concerned about my safety.
 Know It I know the laws of copyright. I know not to bring personal technology to school.	I will use the school email, Purple mash or Google Classroom for any homework if it needs to be sent electronically and not bring a USB stick into school. I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence. I understand the rules of copyright and know I must change things into my own words. I understand that I should not bring my own technology to school and if I do (for an agreed purpose) I must give it to my teacher to keep until the end of the day.

Appendix B: Acceptable Use Policies for Staff

Skirlaugh CE Primary School

‘a caring Christian learning community where everyone is valued’

Acceptable Use Policy for Adults in School

This document has been developed to ensure staff within school are aware of their professional responsibilities when using ICT equipment and systems. This document should be read in conjunction with the Online Safety policy. Staff should follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity which involves using ICT equipment and information systems, either within school or at other locations, such as home. ICT equipment and associated technologies include all facilities and resources used to access the school ICT network and internet as well as standalone devices with digital storage.

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.
- I will access the internet and other ICT systems using a personal staff login and password. I will ensure that I log out after each session. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the Online Safety coordinator.
- All passwords I create will be in accordance with the Online Safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems and that I will use a unique password for each system.
- I will not share my passwords with any pupils within school.
- I will seek consent from the Online Safety coordinator/ Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the Online Safety coordinator/ Headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the network manager / Online Safety coordinator.
- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's GDPR 2018 Data Protection Policy and any information-handling procedures both on and off site.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will act responsibly with any equipment taken off site for school trips.

- I will only use school-owned or provided portable storage (i.e. encrypted USB sticks). I understand that it is an offence to have sensitive/confidential information on USB sticks that are not encrypted, and if found to be in breach of GDPR regulations could lead to prosecution.
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the network manager/Online Safety coordinator.
- I will return any school-owned ICT equipment or software to the SBM once it is no longer required.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.

Social Media

- I will not talk about my professional role in any capacity when using personal social media such as Facebook, X (formerly Twitter) and YouTube or any other online publishing websites.
- I will not use any social media tools to communicate with parents unless approved in writing by the Headteacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- I will not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the Online Safety coordinator.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. 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. No resources will be published online without the permission of the staff and pupils involved as detailed in the Online Safety Policy.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff ie Online Safety coordinator or Head Teacher.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and immediately deleted from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning and teaching

- I will support and promote the Online Safety Policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.
- I will ensure that any use of AI within the classroom will be carefully considered and assessed, evaluating the benefits and risks of use. The use of AI will be in line with the DFE guidance and policy for AI.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I will ensure that I manage my email account, delete sensitive emails and file those I need to keep in subject folders or on an encrypted stick.
- I will access my school email account on a regular basis to ensure that I read and respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode and kept out of sight of the children during school hours.
- I will not contact any parents or pupils on my personally-owned device, unless in an emergency.
- I will not use any personally-owned mobile device to take images, video or sound recordings, unless in unforeseen/emergency circumstances or this has been agreed with the headteacher in advance.
- I will not use any personally-owned mobile device to connect to the school's wi-fi.

Agreement

I have read and understand all of the above listed points relating to my use of technology within school. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Signed:

Print name:

Date: