

Grindleton C.E. Primary School



Online Safety Policy

The following policy is routed in our school's Christian Vision:

As a unique village school, inspired by our Christian love, we strive to nurture our family to 'grow and shine in God's glory'. We will open our hearts to God's wonderful, diverse creation cherishing everyone as a child of God. Through Jesus' example, we will instil resilience and confidence for tomorrow.

'In the same way, let your light shine before others that they may see your good deeds and glorify your father in heaven.' Matthew 5 v16

Key Details

Designated Safeguarding Lead: (Paul Holden)

Back-up Designated Safeguarding Lead: (Hilary Walmsley)

Named Governor with lead responsibility: (Shirley Bush)

Date written: (February 2022)

Date agreed and ratified by Governing Body: (March 2022)

Date of next review: (September 2022)

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

Contents

	Page number
1. Policy Aims	4
2. Policy Scope	4
3. Schools Roles and Responsibilities	5
o 3.1 The leadership and management team	5
o 3.2 The Designated Safeguarding Lead	5
o 3.3 Members of staff	6
o 3.4 Learners	6
o 3.5 Parents	6
4. Education and Engagement Approaches	6
o 4.1 Education and Engagement with Learners	6
o 4.2 Vulnerable Learners	7
o 4.3 Training and Engagement with Staff	7
o 4.4 Awareness and Engagement with Parents and Carers	8
5. Reducing Online Risks	8
6. Safe use of technology	8
o 6.1 Classroom use	8
o 6.2 Managing Internet Access	9
o 6.3 Filtering and Monitoring	9
o 6.3.1 Decision Making	9
o 6.3.2 Filtering	9
o 6.3.3 Monitoring	10
o 6.4 Managing Personal Data Online	10
o 6.5 Security and Management of Information Systems	10
o 6.5.1 Password Policy	10
o 6.6 Managing the Safety of our Website	11
o 6.7 Publishing Images and Videos Online	11
o 6.8 Managing Email	11
o 6.8.1 Staff Email	11
o 6.8.2 Learners' Email	11
o 6.8.3 Content	12
o 6.9 Management of Applications used to Record Children's Progress	12
7. Social Media	12
o 7.1 Expectations	12
o 7.2 Staff Personal Use of Social Media	13
o 7.3 Learners Personal Use of Social Media	14
o 7.4 Official Use of Social Media	14
8. Use of Personal Mobile Phones	15
o 8.1 Expectations	16
o 8.2 Staff Use of Personal Devices and Mobile Phones	16
o 8.3 Learners Use of Personal Devices and Mobile Phones	17
o 8.4 Visitors' Use of Personal Devices and Mobile Phones	17
9. Responding to Online Safety Incidents and Concerns	17
o 9.1 Concerns about Learners' Welfare	18
o 9.2 Staff Misuse	18
10. Procedures for Responding to Specific Online Incidents or Concerns	18
o 10.1 Online Sexual Violence and Sexual Harassment between Children	18
o 10.2 Youth Produced Sexual Imagery (Sexting)	19
o 10.3 Online Child Sexual Abuse and Exploitation (including CCE)	20
o 10.4 Indecent Images of Children	21
o 10.5 Cyberbullying	22
o 10.6 Online Hate	22
o Online Radicalisation and Extremism	22
11. National Links and Resources	23
12. Acceptable Usage for staff, Governors and regular visitors	24
13. Acceptable Use Policy – Supply Teachers and Visitors/Guests Agreement	26
14. Acceptable Use Policy and Online Safety Rules for Pupils	27
15. Acceptable Use Policy – letter to parents	28
16. Online Safety Incident Log	29

1. Policy Aims

- This online safety policy has been written by Grindleton C.E. Primary School involving staff, learners and parents/carers
- It takes into account the DfE statutory guidance [Keeping children safe in education 2021](#), [Early years foundation stage \(EYFS\) statutory framework 2021](#), and the [Working Together to Safeguard Children 2018](#).
- The purpose of Grindleton C.E. Primary School online safety policy is to:
 - Safeguard and protect all members of Grindleton C.E. Primary School 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.
 - Identify clear procedures to use when responding to online safety concerns.
- Grindleton C.E. Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three 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.

2. Policy Scope

- Grindleton C.E. Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Grindleton C.E. 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.
- Grindleton C.E. Primary School believes that learners 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, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.1 Links with other policies

- Anti-Bullying
- Acceptable Usage Policy
- Behaviour Management Policy
- Safeguarding and Child Protection Policy
- Social Media Policy
- Code of Conduct
- Prevent Duty Policy

3. Schools Roles and Responsibilities

- Mr Paul Holden (Headteacher) has overall responsibility to ensure the policy is embedded and adhered to but the policy was also developed in conjunction with the Computing Lead (Miss Woodvine) and The Designated Safeguarding Lead (DSL) (Mr Holden/Headteacher) and the back-up DSL Mrs Walmsley/Assistant Headteacher).
- Grindleton C.E Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

3.1 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 staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within the PSHE curriculum (PHSE Association), which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the 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.

3.2 The Designated Safeguarding Lead (DSL) 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.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- 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 settings 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 Governing Body.
- Review and update online safety policies on a regular basis (annually) with stakeholder input

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

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting 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 possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally

3.4 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- 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.

3.5 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. Education and Engagement Approaches

4.1 Education and engagement with learners

The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The setting will support learners to read and understand the acceptable use of policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Ensure that differentiated and ability appropriate online safety education, access and support is provided to all learners including vulnerable learners. (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.)
- Providing online safety education and training as part of the transition programme across the key stages
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

4.2 Vulnerable learners

- Grindleton CE Primary School recognises that some learners are 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.
- Grindleton CE Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners
- When implementing an appropriate online safety policy and curriculum Grindleton CE Primary School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

4.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures 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 during the safeguarding updates and regularly throughout the year.
- This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

4.4 Awareness and engagement with parents and carers

- Grindleton CE Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We 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.
 - Drawing their attention to the online safety policy and expectations on our website.
 - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
 - Requiring them to read our acceptable use policies and discuss the implications with their children.

5. Reducing Online Risks

- Grindleton 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 the setting 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 our computers or devices.
- All members of the community are made aware of our 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 our acceptable use policies and highlighted through a variety of education and training approaches.

6. Safer use of technology

6.1 Classroom Use:

- Grindleton C.E. Primary School uses a wide range of technology. This includes access to:
 - Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be monitored closely by a teacher or teaching assistant.

Key Stage 2

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learner's age and ability.

6.2 Managing Internet Access

- All staff, learners and visitors will read and sign an acceptable use policy (at the end of this policy) before being given access to our computer system, IT resources or internet.
- We will maintain a written record of users who are granted access to our devices and systems. An acceptable usage policy will be kept on file.

6.3 Filtering & Monitoring

6.3.1 Decision Making

- Grindleton C.E. Primary School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by advice from BTLS
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

6.3.2 Filtering

- Education broadband connectivity is provided through BTLS.
- We use Netsweeper which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. We work with BTLS/Netsweeper to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
 - Report the concern immediate to a member of staff.
 - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or Back-up).
 - The breach will be recorded and escalated as appropriate.
 - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Lancashire Police or CEOP.

6.3.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by regular checking of reports provided by the filtering company to check to inappropriate use.
- If a concern is identified via monitoring approaches we will:
 - Investigate the incident and ascertain individual responsible
 - Inform the parents and follow the Behaviour Policy
 - Contact the local police and request a visit.
 - Review the policy
 - Check the filtering systems
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

6.4 Managing Personal Data Online

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

6.5 Security and Management of Information Systems

- We take 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 using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on our network
 - The appropriate use of user logins and passwords to access our network.
 - 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 at:
 - Acceptable Usage Policy
 - Social Media Policy
 - Staff Code of Conduct
 - Staff Induction Policy

6.5.1 Password Policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- Each class is provided with a username and password
- All learners are provided with their own unique username and private passwords to access their learning on the computers (Seesaw, Purple Mash, Numbots, TT Rockstars)
- Learners are responsible for keeping their password private.

6.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We 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 learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

6.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

6.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
 - The forwarding of any chain messages/emails is not permitted.
 - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email by the HT or SBM.
 - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL or Back up DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Emails are managed by the Head Teacher.

6.8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
 - All members of staff are provided with an 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, learners and parents.

6.8.2 Learner email

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy 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 setting.

6.8.3 Content

- If recording a videoconference lesson, it should be made clear to all parties at the start of the conference, the reason for the recording must be given and recorded material will be stored securely.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.
- A visitor may be invited onto the Learning Platform (Zoom) by a member of staff.

6.9 Management of Applications (apps) used to Record Children's Progress

We use Tapestry to track learner's progress in EYFS. The Data Protection is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

- To safeguard learner's data:
 - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
 - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
 - Devices will be secured appropriately 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.

7. Social Media

7.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Grindleton C.E. Primary School community.
- The term social media may include (but is not limited to): social networking sites blogs; wikis; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Grindleton C.E. Primary School community are expected to engage in social media in a positive, safe and responsible manner.
 - All members of Grindleton C.E. Primary School 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.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site

- The use of social media during teaching time for personal use is not permitted.
 - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Grindleton C.E. Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

7.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites was discussed at a staff meeting on the setting up of our Facebook and Twitter sites. It is discussed as part of staff induction and will be revisited and communicated where appropriate.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
 - Civil, legal or disciplinary action may be taken if staff 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.
 - 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 setting.
- All members of staff are encouraged not to identify themselves as employees of Grindleton C.E. Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and 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 our 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 learners and their family members or colleagues will not be shared or discussed on social media sites.
 - Members of staff will notify the DSL or Back up DSL immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their 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 the head teacher.
 - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the head teacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or Back-up).

7.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
 - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners 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.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
 - 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.
 - How to report concerns both within the setting and externally.

7.4 Official Use of Social Media

- Grindleton CE Primary School official social media channels are:
 - Twitter
 - Facebook
- The official use of social media sites 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 head teacher.
 - Leadership staff has access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use setting provided email addresses (head@) to manage official social media channels.

- Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
- Public communications on behalf of the setting 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/camera 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 learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
 - Only social media tools (which have been risk assessed and approved as suitable for educational purposes will be used.
 - Any official social media activity involving learners will be moderated possible
- Parents and carers will be informed of any official social media use with learners.
- We 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.
- Any child with negative consent for Social Media photos will be removed/obscured from images.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional 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 setting, they will:
 - Always be professional and aware they are an ambassador for the setting.
 - Disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the setting.
 - Always be responsible, credible, fair and honest, 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 consent before sharing images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
 - Inform their line manager, the DSL (or Back-up) *and/or* the *head teacher* of any concerns, such as criticism, inappropriate content or contact from learners.

8 Use of Personal Devices and Mobile Phones

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

Learners will not be allowed to bring mobile phones into school without prior permission from the Head Teacher. If a learner brings a device into school it will be kept in the school office until the end of the day.

8.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
 - All members of Grindleton CE Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - All members of Grindleton CE Primary School 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 may be used in the staff room for personal calls and messages.
- The sending of abusive or inappropriate messages or 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 Grindleton CE Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

8.2 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 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 (**in staffroom or located away from children in the classroom**) during lesson time.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods, unless permission has been given by the head teacher, such as 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 learners or parents and carers.

- Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or Back-up).
- Staff will not use personal devices:
 - To take photos or videos of learners and will only use work-provided equipment for this purpose.
 - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff 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.

8.3 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Grindleton CE Primary School does not allow personal devices in school and any devices should be handed to the office on entering school.
- If a learner needs to contact his/her parents or carers they will be allowed to use the office phone.
- Parents are advised to contact their child via the setting office

8.4 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 our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and 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 DSL (or Back-up) or *head teacher* of any breaches our policy.

9 Responding to Online Safety Incidents and Concerns

- All members of the 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 procedures for reporting concerns.
 - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or Back-up) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Lancashire Police using 101, or 999 if there is immediate danger or risk of harm.

- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL (or Back-up) speak with Lancashire Police *and/or* the Education Safeguarding Team first to ensure that potential investigations are not compromised.

9.1 Concerns about Learners Welfare

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

9.2 Staff Misuse

- Any complaint about staff misuse will be referred to the head teacher, in accordance with 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 our staff behaviour policy/code of conduct.

10 Procedures for Responding to Specific Online Incidents or Concerns

10.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting follows the guidance of "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2021.
- Grindleton CE Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
 - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection safety.
- Grindleton CE Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Grindleton CE Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Grindleton CE Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. We will ensure that all members of the community are aware of sources (links at the bottom of this policy and links on the safeguarding section of the website) of support regarding online sexual violence and sexual harassment between children.

- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
 - Immediately notify the DSL (or Back-up) and act in accordance with our child protection and anti-bullying policies.
 - If content is contained on learner's electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
 - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
 - Implement appropriate sanctions in accordance with our behaviour policy
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
 - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
 - If a criminal offence has been committed, the DSL (or Back-up) will discuss this with Lancashire Police first to ensure that investigations are not compromised.
 - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

10.2 Youth Produced Sexual Imagery ("Sexting")

- Grindleton CE Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or Back-up).
- We 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".
- Grindleton 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.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We 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.
 - If it is deemed necessary, the image will only be viewed by the DSL (or Back-up DSL) 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 a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
 - Act in accordance with our child protection policies and the relevant Lancashire Safeguarding Child Board's procedures.
 - Ensure the DSL (or Back-up) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
 - Store the device securely.
 - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners 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 Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise 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 DSL 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.

10.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Grindleton 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.
- Grindleton CE Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or Back-up).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community via our website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
 - Act in accordance with our child protection policies and the relevant Lancashire Safeguarding Child Board's procedures.
 - If appropriate, store any devices involved securely.

- Make a referral to Children’s Social Work Service (if required/appropriate) and immediately inform Lancashire police via 101, or 999 if a child is at immediate risk.
 - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
 - Where possible, learners 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 we are unclear whether a criminal offence has been committed, the DSL (or Back-up) will obtain advice immediately through the Education Safeguarding Team and/or Lancashire Police.
 - If 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 DSL (or Back-up).
 - If learners at other setting are believed to have been targeted, the DSL (or Back-up) will seek support from Lancashire Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

10.4 Indecent Images of Children (IIOC)

- Grindleton 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).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) implementing appropriate filtering, firewalls and anti-spam software (BTLS).
- If we are unclear if a criminal offence has been committed, the DSL (or Back-up) will obtain advice immediately through Lancashire Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:
 - Act in accordance with our child protection policy and the relevant Lancashire Safeguarding Child Boards procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as Lancashire police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - Ensure that the DSL (or Back-up) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the appropriate authorities.
 - 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 setting provided devices, we will:
 - Ensure that the DSL (or Back-up) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the appropriate authorities.
 - 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 Work Service (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 setting provided devices, we will:
 - Ensure that the *head teacher* is informed in line with our managing allegations against staff policy.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
 - Quarantine any devices until police advice has been sought.

10.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Grindleton CE Primary School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

10.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Grindleton CE Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or Back-up) will obtain advice through the Education Safeguarding Team and/or Lancashire Police.

10.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or Back-up) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the head teacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

11. National Links and Resources for Educational Settings

- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Grindleton CE Primary School

12. ICT Acceptable Use for Staff and Governors and regular visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual/professional responsibilities when using any form of ICT. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally
- I will be an active participant in Online Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
- I will not use communications devices, where school provided or personally owned, for bullying or harassment of others in any form.
- I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites Forums and Chat rooms.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights
- I will ensure that all electronic communications with pupils and other adults are appropriate.
- I will not use the school system(s) for personal use during working hours
- I will not install any hardware or software without the prior permission of the Headteacher
- I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with the Data Protection legislation.
- I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer or person/s in the image.
- I will report any known misuses of technology including the unacceptable behaviour of others
- I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services
- I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date

Full name (PRINT)

Position/Role

Grindleton CE Primary School

13. ICT Acceptable Use Policy – Supply Teachers and Visitors/Guests Agreement

For use by any adult working in the school for a short period of time.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will respect copyright and intellectual property rights.
- I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission for the parent/carer or person/s in the image.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date

Full name (PRINT)

Position/Role.....

Grindleton CE Primary School

14. ICT Acceptable Use and Online Safety Rules for Pupils

- I will only use ICT (for example: computers, iPad, cameras etc.) in school for school purposes.
- I will only use the internet and/or online tools when a trusted adult is present
- I will only use my class email address when emailing
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home
- I will not deliberately look for, or access inappropriate websites
- If I accidentally find anything inappropriate I will tell my teacher immediately
- I will only communicate online with people a trusted adult has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others' details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords
- I will not arrange to meet anyone that I have met online
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my Online Safety.
- I understand failure to comply may result in disciplinary steps being taken in line with the School's Behaviour Policy.

Parent/Carer Signature

We have discussed this Acceptable Use Policy and (Child's name) agrees to follow the Online Safety rules and to support the safe use of ICT at Grindleton CE Primary School.

Signed Parent/Carer.....Please Print

Pupil's Name.....Date

Grindleton CE Primary School

15. ICT Acceptable Use Policy – Parent’s Letter

Dear Parent/Carer

The use of ICT including the Internet, e-mail, learning platforms and today’s mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside, of the school environment.

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy document forms part of the wider School Online Safety Policy and alongside the school’s Behaviour Policy outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed document with your child and return as soon as possible.

If you have any concerns or would like to discuss any aspect of the use of ICT in school please make an appointment and will be happy to discuss this with you.

Yours faithfully

Mr P Holden
Headteacher

GRINDLETON CE PRIMARY SCHOOL**16. Online Safety Incident Log**

All Online Safety incidents must be recorded by the Headteacher as.
This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors.

Date/Time of incident	Type of Incident	Name of pupil/s and Staff involved	System details Incident details	Actions taken and by whom