Grindleton CE Primary School

E-Safety Policy Statement

Contents

Introduction

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

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

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

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones/tablets with text, video and/ or web functionality
- Other mobile devices with web functionality

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

At Grindleton CE Primary School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

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

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, Mrs Stansfield (headteacher) will have ultimate responsibility to ensure that the policy and practices are embedded and monitored. However, certain responsibilities may need to be delegated to other staff as the Headteacher feels is necessary. All members of the school community have been made aware of who holds this post. It is the role of the eSafety leader to keep abreast of current issues and guidance.

Senior Management and Governors are updated by the Head and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

eSafety skills development for staff

- Our staff receive regular information and training on eSafety issues in the form of meetings, inset and briefings
- Details of the ongoing staff training programme can be found in staff meeting minutes.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All teaching staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community, (see appendix 1).
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.

Managing the school eSafety messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- The eSafety policy will be reintroduced to the pupils at the start of each school year in the form of an eSafety awareness session.
- ESafety posters will be prominently displayed in all classrooms.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing and PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline / CEOP report abuse button.

Data Security

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Lancashire Grid For Learning (LGFL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Lancashire Local Authority has a monitoring solution via the Lancashire Grid for Learning where web-based activity is monitored and recorded.
- School internet access is controlled through the Lightspeed Systems.
- Grindleton Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.

- If staff or pupils discover an unsuitable site, the screen must be switched off and the incident reported immediately to the eSafety leader.
- It is the responsibility of the school, by delegation to Schools-IT UK Limited, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility, nor that of Schools-IT UK Limited, to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without consulting eSafety leader
- If there are any issues related to viruses or anti-virus software, the eSafety leader should be informed.

<u>Managing other Web 2 Technologies</u>

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavour to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher such as the school's website, twitter feed or Facebook page.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. These must be used in their own time, away from the children. Otherwise, these must be switched to silent and out of sight of pupils, unless permission is given by the Headteacher.
- Under no circumstances, except in an emergency, does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school but if family circumstances are such, then they must not use them for personal purposes during the school opening hours. At all times the device must be switched onto silent and left in the care of the class teacher.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing E-mail

The use of email within most schools is an essential means of communication, although, in the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. The key learning documents produced by Lancashire also state that children should begin to develop their understanding of emails from years 1 and 2.

- The school gives all staff, who request it, their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations or parents, are advised to cc. the Headteacher, line manager or designated account where it is deemed necessary.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- No children have individual school issued accounts, children use a class/group email address when necessary.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.
- Staff must inform (the eSafety leader) if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing curriculum

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils ONLY with school equipment. No other adult or child is permitted to take images of staff or pupils, unless given the express permission of the Headteacher.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

- Twitter feed
- Facebook page

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by the main carer in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the teachers have the authority to choose the content to upload to the site.

Storage of Images
- Images/ films of children are stored on the school's network, laptops and cameras, which are password protected.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- Images are stored on an external hard-drive and kept in a secure cupboard when not in use.
- All teaching staff have the responsibility of deleting the images when they are no longer required.

Webcams and CCTV
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, e.g. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (See appendix 3).

Video Conferencing
- Currently, the school does not have video conferencing equipment, however if this is purchased:
- Permission is sought from parents and carers if their children are involved in video conferences.
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing.

- All pupils are supervised by a member of staff when video conferencing with endpoints beyond the school.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Misuse and Infringements

All incidents relating to the misuse of technology shall be recorded in an Incident Log which will be reviewed by Headteacher and governors on a regular basis.

Illegal offences
Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Staff must never personally investigate, interfere with or share evidence as they may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix 3)

Potential illegal content is reported to Internet Watch Foundation (http://www.iwf.org.uk) as they are licensed to investigate. Examples of illegal offences are:
- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

Equal Opportunities

Pupils with additional needs
The school endeavour to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss eSafety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by parent discussion group, school council.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of; Information evenings, Posters o Website/ 'Learning Platform' postings, Newsletter items, 'Learning Platform' training.

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation

- Staff and pupils have been involved in making/ reviewing the eSafety policy through staff meetings and discussions with pupils during PHSE.

Review Procedure
There will be an on-going opportunity for staff to discuss with the eSafety Leader any issue of eSafety that concerns them. This policy will be reviewed every twelve months and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Signed on behalf of the

Governors: _____   Date: _____

Date to be reviewed: _____Spring Term 2020_____

Grindleton CE Primary School

Image Consent Form

Name of child (in full) :- ………………………………………………………

We regularly take photographs/videos of children at our school and permission is required so we can use them:-

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

In order that we can protect your child's interest, and to comply with the Data Protection Act (1998), please read the Conditions of Use on the back of this form.
Please sign, date and return the completed form (one for each child) to school as soon as possible.

I have read and understand the conditions of use on the reverse of this form.

Signature of Parent/Carer ………………………………………. Date…………………..

Please print …………………………………………………

Conditions of Use

1. This form is valid for the entire period that your child attends Grindleton CE Primary School.
2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.
3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.
4. If we use photographs of individual pupils, we will not use the full name of that pupil in any accompanying text or caption.
5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.
6. We will only use images of pupils who are suitably dressed.
7. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies
8. Before posting student work on the Internet, a check will be made to ensure that permission has been given for work to be displayed. Only the teachers have the authority to choose the content to upload to the site.

Notes on Use of Images by the Media

If you give permission for your child's image to be used by the media then you should be aware that:

1. Pupils' names will not be published alongside their image and vice versa. 2. E-mail and postal addresses of pupils will not be published.
3. Pupils' full names will not be published.

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, responsibility and legally
- I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
- I will not use communications devises, 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 eSafety 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

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, responsibility 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 fo 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

ICT Acceptable Use and eSafety 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 eSafety.
> ➢ 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 eSafety 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

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 responsibility 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 eSafety 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

e-Safety Incident Log

All eSafety incidents must be recorded by the Headteacher as eSafety Champion. 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