Approved by Governors (date)………………………

Head Teacher…………………….............

On behalf of Governors ……………………………

CASTLE VIEW PRIMARY AND NURSERY SCHOOL
E-SAFETY/ACCEPTABLE USE POLICY

The member of school responsible for E-safety is Jennifer Ord.
All members of the school community should agree to an 'Acceptable Use Policy' that is appropriate to their age and role.
Appendix 1:AUP policy for staff/governors/visitors
Appendix 2:AUP policy for KS1 and KS2
Appendix 3: AUP sent to parents
The AUP will form part of the first lesson of ICT for each year group.

Introduction

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 to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology 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. Currently, the internet technologies children and young people are using both inside and outside the classroom include:

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

Whilst exciting and beneficial (both in and outside 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.
We understand the responsibility to educate our pupils on E-safety issues; teaching them the appropriate behaviours 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 utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

The Prevent Duty

The Prevent Duty is the duty in the Counterterrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff need to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns of overuse of the internet that includes, for example, the following:

- Internet searches for terms related to extremism.
- Visits to extremist websites.
- Use of social media to read or post extremist material.
- Grooming of individuals.

The Prevent Duty requires a school's monitoring and filtering system to be fit for purpose.

Roles and Responsibilities

As E-safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named E-safety Co-ordinator in our school is Jennifer Ord and they have been designated to this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the E-safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Headteacher or E-safety Co-ordinator and all Governors understand 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, Behaviour (including the anti-bullying) Policy and PHSE.

E-safety skills development for staff

- Our staff receive regular information and training on E-safety issues in the form of regular staff training.
- New staff receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-safety and know what to do in the event of misuse of technology by any member of the school community. (See attached flowchart.)
- All staff are encouraged to incorporate E-safety activities and awareness within their curriculum areas.

Managing the school E-safety messages

- We endeavour to embed E-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-safety Policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.

E-safety in the Curriculum

- Castle View implement a specific E-Safety curriculum that is separate to the Computing curriculum. This is taught both in Computing lessons, in the wider curriculum, in PSHE lessons and in school assemblies.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety Curriculum.
- E-safety awareness days are held in the Spring and Summer terms and are a focus each year in line with the UK Safer Internet Centre and the Internet Safety Day they promote.
- 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.
- Trips and visitors are planned for throughout the year to provide further opportunities for educating our young people about staying safe online and offline, such as Police Talks on internet safety, Crucial Crew, Safety Central.

Passwords and Security

- Passwords should be changed regularly.
- Passwords must not be shared.
- Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and allow a PC to be 'locked').
- All users should be aware that the ICT system is filtered and monitored.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-safety Policy.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers, or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, SIMS MIS system.
- In our school, all ICT password policies are the responsibility of the Headteacher, and all staff and pupils are expected to always comply with the policies.

Data Security

The accessing of school data is something that the school takes very seriously.
Staff are aware of their responsibility when accessing school data. They must not,

- allow others to view the data,
- edit the data unless specifically requested to do so by the Headteacher.

Managing the Internet

The internet is an open communication medium, available to all, always. 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.

- Pupils will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are only carried out by pupils under supervision.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must always observe software copyright. 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.
- You tube will be accessed by teachers only within a classroom situation.
- Teachers must search for and identify the appropriate clip before the children are asked to watch.
- Skype is to be used only as a whole class activity lead by a member of staff.

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with 24/7 Technology Ltd.

Managing filtering

The school will work with the 24/7, LEA, DFES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the E-safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.

INFRASTRUCTURE

System Managed by BMITS Remotely and onsite, also ICT-Coordinator has access for blocking and unblocking with Headteacher's authorisation.

ICT-Coordinator can access and block site or sites at the time or BMITS can block instantly via Remote Access.

- The school is aware of its responsibility when monitoring staff communication under current legislation and considers; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights 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/ closed and the incident reported immediately to the E-safety Co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up to date on all school machines.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher.

Managing other Web 2 technologies (social media/blogs/YouTube etc)

Web 2/Social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative 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 endeavours to deny access to social networking sites to pupils within school. It is also noted that the age of the children would suggest that they are too young to sign up to social networking sites but may have access to them. Therefore, all the advice and teaching are given in context of being SMART on line.
- 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, IM/ 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 parents/pupils in line with school software choices e.g., school blog/twitter.

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 school too. They often provide a collaborative, well-known device with possible internet access and thus invite 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/smartwatches)

- The school allows staff to bring in personal mobile phones and devices for their own use. Only under exceptional circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. For example, when a trip is outside normal school hours/residentials. The person making the call should endeavour to keep their number private by withholding their number.
- Pupils are not allowed to bring personal mobile devices/phones to school/wear smartwatches which support phone and camera style technologies, unless with the prior approval of the school. Those who do, must leave them in the care of their teacher in a labelled bag at the beginning of the day and collect them at end of the day. Pupils' phones must be password protected and switched off for the duration of the time they are in school.
- The school is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate text messages or emails between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices

- The sending of inappropriate text messages between any member 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 school.

Use of Mobile Phones for Volunteers and Visitors

- When entering the building, there is a sign which states that mobile phones should be switched off.

- If visitors wish to make or take an emergency call, they may use either the main or the manager's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

Managing email

The use of email within most schools is an essential means of communication for staff. 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'.

- Children are taught how to write and send an email using a secure learning platform which is regularly monitored. These emails can only be sent to registered users within the school.
- Staff have a school email account which should be used for school related emails and for planning.
- Any e-mails containing confidential information will be transferred only by the school's secured e-mail account.
- The Senior Leadership Team and Administration Staff are responsible for the sending of emails through the secure account.
- 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, so that necessary email histories can be traced.
- 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 secure 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 are advised to cc. the Headteacher, Line Manager or Designated Account.
- The forwarding of chain letters, this includes jokes and funny statements, 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.
- Staff must inform the E-safety Co-ordinator/ line manager if they receive an offensive e-mail.

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 with school equipment.
- If photos/videos are to be used online, then names of pupils should not be linked to pupils.
- Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils.
- 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.
- Photos taken by the school are subject to the Data Protection Act.
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

- Parents attending school-based events will be reminded of their responsibilities in relation to social media verbally and through notices.
- The parental letter concerning AUP’s includes a paragraph concerning posting photographs on social networking sites.
- Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

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 virtual learning platform
- on the school web site
- on the school blog
- on the school’s social media accounts
- 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)

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. 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.

Data storage

- Only encrypted USB pens are to be used in school.
- Staff should endeavour to save and store data on the school’s cloud based, password protected system.

Storage of Images

- Images/ films of children are stored on the school’s network.
- 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.
- Images are stored on the cloud and deleted when necessary.

Webcams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school will only ever used for specific learning purposes, i.e., 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 (as listed under the ‘inappropriate materials’ section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.
- CCTV is used on the school grounds for monitoring purposes.

Video Conferencing

- 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 endpoints outside 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 will keep 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.

Use of Social Media

- Teaching and Administration staff have access to the school's social media sites but must use it in accordance with the policy.
- Images and videos uploaded onto the social media accounts must not name pupils and should only be of pupils whose parents have given consent.
- Staff must ensure that social media platforms are used solely for providing information to parents about school events or learning that has taken place.
- Pupils are not permitted to use social networking sites within school.

Reporting

All breaches of the E-safety Policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Lead immediately – it is their responsibility to decide on appropriate action not the class teacher's.

Incidents that are of a concern under the Prevent Duty should be referred to the Designated Lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g., cyberbullying) should be reported to Alicia Sheady on the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g., CEOP button, trusted adult, ChildLine).

Misuse and Infringements

Whenever a student infringes the E-safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-safety Co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-safety Co-ordinator, depending on the seriousness of the offence; investigation by

the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

- Users are made aware of sanctions relating to the misuse or misconduct by formal interview and follow up letter from the Headteacher.

Pupils with additional needs

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

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

Parental Involvement

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school E-safety policy by discussion through information events and annual questionnaires.
- 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 decide as to whether they consent to images of their child being taken/used in the public domain (e.g., on school website).
- When children are learning remotely, it is the responsibility of the parents/carers to monitor what children are accessing online.
- Parents/carers will support the school to ensure only the named child accesses the School's Virtual Learning Platforms.
- Parents/carers will support school to ensure the school's Virtual Learning Platform contents are not shared with anyone else or shared on any other platform.
- The school will support parents/carers by disseminating information to parents relating to E-safety where appropriate in the form of,

o Information and celebration evenings
o Posters
o Website
o Blog posts
o Social media posts
o Newsletter items

Review Procedure

There will be an on-going opportunity for staff to discuss with the E-safety coordinator any issue of E-safety that concerns them.

This policy will be reviewed annually, 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.

Reviewed September 2022

Next review: September 2023

Appendix 1: Castle View Primary School

Acceptable Use Agreement/ Code of Conduct: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and always adhere to its contents.

Any concerns or clarification should be discussed with the school E-safety coordinator.

- I will only use the school's email / Internet / Intranet / social media/ phones and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils or parents.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher.
- I will not install any hardware or software without permission of the Headteacher.
- I will not browse, download, upload, or distribute any material that could be considered offensive, illegal, or discriminatory.
- Images of pupils and/ or staff will only be taken, stored, and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..………………….………… Date ……………………

Full Name ………………………………..(printed)

School…………………………………………………………………

Job title . . . .

Appendix 2 – Acceptable Use Policies

Acceptable Use Policy for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger
- not share any information from the school's Virtual Learning Platform

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name ……………………………….......................................(printed)

Date ……………………

Appendix 2 – Acceptable use Policy
Acceptable Use Policy for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate for my learning purposes
- respect the school network and equipment
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- keep the computer equipment on a flat surface
- follow class rules when using the equipment such as taking turns, passing iPads carefully
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only use email which has been provided by school
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me
- put equipment back gently and make sure the iPads go on charge
- only edit your own work
- if taking photographs, always ask others for their permission first (only take photographs if your teacher has allowed it)
- follow the SMART rules when using the internet. (safe, meeting, accepting, reliable, tell)
- encourage others to follow the rules
- not share any information from the school’s Virtual Learning Platform

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……..…………………….………… Date ……………………

Full Name …………………………………...(printed)

Appendix 3 – Parent letter – internet/e-mail use

Castle View Primary School

Parent / guardian name: …………………………………………………………...

Pupil name: …………………………………………………………………

Pupil's registration class: ……………………………………

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed if the rules must be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching E-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's E-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's E-safety.

I accept that my child will follow school policies for appropriate use when using Internet based services. Pupils are provided with an account linked to our school's Virtual Learning Platform. I understand that this school learning platform is only for the named child to use and the content should not be shared with anyone else or shared on any other platform.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to E-safety and will not upload or add any pictures, video or text that could upset, offend, or threaten the safety of any member of the school community.

Parent / Guardians' signature: ……………………………………………

Your name (in block capitals): …………………………………………….

Date: …………………. …..