COLD HARBOUR
C of E Primary School

Growing, Learning, Achieving Together

E-safety and acceptable use policy 2017

Responsibility of Curriculum Committee

Next Review Date:

	Date	Signature
Discussed at Staff meeting	**22.11.17**	
Discussed at Curriculum Governors meeting	**16.01.18**	
FGB:	**22.03.18**	

Cold Harbour CE Primary School
Policy Ethos Statement

Ensuring that our children have every opportunity to develop the confidence and capacity to become successful, lifelong learners is a key task for us.

Cold Harbour CE Primary School is a school committed to 'Growing, Learning, Achieving Together' with strong Christian values underpinning this.

- ü Growing in confidence, faith, personal awareness and ability.
- ü Learning in creative, fun, technologically assisted and investigative ways.
- ü Achieving as individuals, teams and as a whole school community across a diverse range of opportunities.
- ü Together through our shared Christian values of tolerance, faith, guidance, respect and nurture.

This policy will clearly define how the procedures and opportunities in school will enable all children to achieve our key aims.

'Do all the good you can,
By all the means you can,
In all the ways you can,
In all the places you can,
At all the times you can,
To all the people you can,
As long as ever you can.'
(John Wesley)

Cold Harbour CE Primary School
E-safety and Acceptable Use Policy

Computing leader – *Ruth Burgess*
E-safety Leader – *Ruth Burgess*
Safeguarding Governor – *Sharon Power*

1. What is an AUP (Acceptable Use Policy)?

The Acceptable Use Policy (AUP) sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies, particularly those on-line, (including the Internet, Class Dojos, E-mail, webcams, Instant Messaging and other social networking spaces, mobile phones, portable media, such as memory sticks and laptops, and games) to safeguard adults and children within the school setting. It also details how Cold Harbour will provide support and guidance to, children, staff, parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies, beyond the school setting. In addition it explains procedures for unacceptable or misuse of these technologies by adults or children.

2. Why have an AUP?

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There will always be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies.

These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- Online content which is abusive, pornographic or inappropriate for a young audience.

It is also important that all adults are clear about the procedures, for example, only contacting, parents, children and young people about homework via a school e-mail address or communication route, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

As part of the Children's Act it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Whilst Cold Harbour acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people are continued to be protected.

Therefore, the involvement of children and young people and parent/carers is also vital to the successful use of online and digital technologies. This policy also aims to inform how parents/carers and children or young people are part of the procedures and how children and young people are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

3. Aims

To ensure the safeguarding of all children within and beyond the school setting by detailing appropriate and acceptable use of all digital and on-line technologies.

- To outline the roles and responsibilities of everyone in the school community.
- To ensure adults and children are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with children, parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

4. How the internet will be used to enhance learning.

- School Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- All Classes will be taught 'Rules for Responsible Internet Use', at the beginning of a school year, and the skills needed in order to use the Internet appropriately. Children in all classes will sign an agreement to use the internet appropriately and responsibly, as they have been taught to.
- Internet access will be planned to enrich and extend learning activities, and pupils will be given clear objectives for all Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Supervision is the key strategy, aimless surfing should never be allowed – pupils should always use the Internet in response to an articulated need.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (E2Bn) via the E-Safety leader.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using information from the internet.

5. Roles and responsibilities of the school:

5.1 Governors, Head teacher, and e-safety subject leader.

It is the overall responsibility of the Headteacher and E-safety subject leader with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe Computing learning environment.
- Time and resources will be provided for the e-Safety Leader and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher and E-safety Leader will inform Governors at Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or Computing) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors will be made aware of e-Safety developments from the Curriculum meetings.

- The Governors **MUST** ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- The e-Safety Governor will challenge the school about having an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using Computing, including:
    - Challenging the school about having:
        - Firewalls
        - Anti-virus and anti-spyware software
        - Filters
        - Using an accredited ISP (Internet Service Provider)
        - Awareness of wireless technology issues
        - A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers. See appendices for example procedures on misuse.

5.2 e-Safety Leader

It is the role of the designated e-Safety Leader (with support from the headteacher) to:

- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and children, in the initial set up of a network, stand-alone PC, staff/children laptops and other internet enabled devices within school *or ensure the technician is informed and carries out work as directed.*
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people, ensuring that children only use computers that are logged in under a child's profile, not the teachers.
- Report issues and update the Headteacher on a regular basis. This will be reported, as necessary, to the Governors' curriculum and standard committee.
- Liaise with the PSHE, Child Protection and Computing leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Annually update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Transparent monitoring of the Internet and on-line technologies – It is the class teacher's responsibility to monitor *the use of the Internet and technologies by the children in their class.*
- Keep and monitor a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. (Shared Google document)
- Work alongside the Computing subject leader/ICT technician to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer and that this is instigated automatically.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

5.3 Staff or adults

It is the responsibility of all adults within the school setting to:

- Ensure that they know who the Designated Person for Child Protection is within school or other setting so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Headteacher immediately, who should then follow the Allegations Procedure.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the E-safety Leader.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through planning and incorporating appropriate lessons into the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in. (computers should be set to lock/log out after a couple of minutes.)
- Ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the e-Safety Leader and E2Bn in order that inappropriate sites are added to the restricted list. (via shared document)
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the accident/incident reporting procedure in the same way as for other non-physical assaults.

5.4 Children and young people

Children and young people are:

- Involved in the review of our Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Taught to use the Internet in a safe and responsible manner through Computing and PSHE.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).
- Required to keep their password secret from peers.
- Ensure that they securely logoff from any website/computer/chromebook or other device they use during the day.

6. Appropriate use by staff or adults

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access the school network and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to the e-safety leader to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

Please refer to appendices for a complete list of Acceptable Rules for Staff.

6.1 In the event of inappropriate use

If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately. The Allegations Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.
In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

7. Appropriate use by children and young people

Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules will be on display and referred to within all classrooms

We want our parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

Further to this, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free. File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using Google Apps/Class Dojo etc. in or beyond school.

Pupils will be actively involved in discussing the acceptable use of on-line technologies and the rules for misusing them.

7.1 In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school or in a setting the following consequences will occur (these will be reviewed by our school council and stakeholders as the policy is updated):

- Any child found to be misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.
- If the misuse constitutes bullying then the anti-bullying policy will be followed.

In the event that a child or young person **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen by using by turning off the monitor/closing the lid of the Chromebook/laptop, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies will be addressed according to the structure outlined above.

Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

8. The curriculum and tools for Learning

8.1Why the Internet and electronic communication use is important.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management and communication functions. Internet use forms part of the statutory curriculum and as such is a necessary tool for learning.
The Internet forms part of everyday society and as such it is every school's duty to prepare its pupils through quality Internet access with the personal tools to evaluate information and to take care. There are benefits to the Internet and planned government initiatives such as :

- Access to world-wide educational resources. (museums or galleries)
- Inclusion in the National Education Network connecting schools together.
- The potential for world-wide educational and cultural exchanges.
- Access to national developments, educational materials and resources to enhance the National Curriculum.
- Exchange of curriculum and assessment data between National bodies.
- Access school assessment, curriculum and personal resources from any location that has an internet connection.
- The facility to extend learning beyond the traditional school building into an electronic environment.

8.2 Internet use

At Cold Harbour we teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through Computing and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave Year 6 :

- Internet literacy (how to navigate safely, conduct safe searches, filter relevant sites and information)
- Making good judgements about websites and emails received.
- How to safely use social networking sites and the age restrictions applicable and reasons for this.
- How to conduct themselves in social forums and public places on the web such as emails, blogs, chat rooms, text messaging.
- Knowledge of risks such as viruses and opening mail from a stranger
- Access to resources that outline how to be safe and responsible when using any on-line technologies eg 'U Think You Know' website
- Knowledge of copyright and plagiarism issues
- File-sharing and downloading illegal content
- Uploading information – know what is safe to upload and not upload personal information
- Where to go for advice and how to report abuse
- The health and safety issues inherent with prolonged use of technology and the importance of taking breaks.

For many lessons and resources on e-safety or we use the www.thinkuknow.co.uk resources for KS1 and KS2, within PSHE and Computing lessons.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team
- Photograph showing their face

Photographs should only be uploaded on the approval of a member of staff and parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy. Photographs of children's faces should only be used with parental permission and should only be associated with the child's first name.

8.2 E-mail use

We have E-mail addresses for children and young people to use as individuals, as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms. Individual E-mail accounts can be traced if there is an incident of misuse.

Staff, children and young people are to use their school issued e-mail addresses for any communication between home and school only. A breach of this will be considered a misuse and will result in consequences.

Parents/carers are encouraged to be involved with the monitoring of E-mails sent although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of E-mails where there are communications between home and school/setting.

8.3 Video-conferencing

Children need to ask for permission from a member of staff or adult to use this facility both in and beyond school and should only undertake video conferencing when supervised by an adult. Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Rules.)

Where children and young people (and adults) may be using a webcam in a family area at home, they should be encouraged have open communications with parents/carers about their use.

Taking images via a webcam will follow the same procedures as taking images with a digital or video camera.

8.4 Mobile phones and other technologies

The use of mobile phones or PDAs will not be allowed in our school, or on school grounds whilst in charge of children. The exception being for emergencies during an after school club, on a trip or residential visit. Children are not permitted to bring mobile phones into school, if they are required to have a mobile phone for out of school use this must be handed into the school office on arrival and collected at the end of the day.

Staff members are not allowed to use their personal numbers to contact children and young people or parents under any circumstances.

It is also our policy to ensure that we educate our children and young people in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

8.5 Video and photographs

The term ‘image’ refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to:

- digital cameras/web cameras/iPads

The sharing of photographs via the school website, weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer and member of staff. A list of parental permission for photographs/videos should be kept in each class register.

Any photographs or video clips uploaded will not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name (although Child Protection Guidance states either a child's name or a photograph but not both.) If it is possible we prefer to have Group photographs rather than pictures of individual children.

Any photographs taken will not be of any compromising positions or in inappropriate clothing, e.g. swimming kit. The photos taken will be for the parents, or for use on the school website, school documentation and displays. Backup copies are kept on the Staff area of the network only and must not be stored on staff laptops, mobile devices or home computers.

8.6 The management and publication of content.
In this age, the use of websites and social media to showcase a school and the work it produces has become extremely popular. However, it does provide opportunities acquiring sensitive and personal data if consideration is not given to the material available. Unlike newspapers, the publication of pupil faces and full names is not acceptable. These published images could be re-used especially if a large image has been used. In addition to this, the publication of names and contact details of staff will be discouraged and where necessary, access to this information will be available via other methods or through a secure portal such as Class Dojo. Parents will have the option to contact teachers through the use of instant messaging via the Class Dojo app. This secure form of communication will only allow parents of current children to contact staff. A review of the effectiveness of this form of communication will take place termly during staff meetings. Only the school's contact details will be published. Staff or pupil contact information will not be published. The Headteacher and Deputy Headteacher will take editorial responsibility and ensure content is accurate and appropriate. At all times, intellectual property and copyright rights will be respected and complied with.

- Under no circumstances is a pupils' full name to be published anywhere on a website especially when it might relate to a photograph.
- Parents will be given the right to 'opt out' of digital publication in any form of their child on the internet.
- The 'opt out' information will be updated annually and records will be kept.
- At all times, the pupils in photographs should, of course, be appropriately clothed.

9. Filtering and safeguarding measures

The E2Bn broadband connection has a filter system (Protex) which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child.

- All children's access via the local network login or Google apps login uses 'Pupil' filter.
- All adult's access via the local network login or Google apps login uses 'Staff' filter

Protex uses URL lists of inappropriate content and block against that list, it also examines page content, hunting out and evaluating words and phrases from a very extensive list of suspect terms. Should a user find a site that they believe should be blocked they can report the site at http://protex.e2bn.org/listrequest.

The E-safety leader will conduct a half termly test of the filter by logging in as a child and attempting to access inappropriate materials.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis. A firewall ensures information about our children and young people and the school cannot be accessed by unauthorised users.

All computer access requires a child login, it is password protected so that the child is only able to access themselves as a user. Children and young people should be taught not to share passwords.

When children first enter a webpage, they are greeted with the safe search website 'http://www.swiggle.org.uk/home'

Children are taught not to use Google to search safely, for information or pictures in school and are encouraged to do the same at home. They are shown how to enable a safer search within Google but are taught about why this does not offer complete protection.

Children will be taught to cover the screen on laptops and chromebooks/tablets etc so that anything accidentally accessed can be covered whilst an adult is informed, but the image/website can be preserved allowing the adult to take action. Hector Protector safety button can still be downloaded from http://hectorsworld.netsafe.org.nz/teachers/hectors-world-safety-button/ but may no longer be compatible with modern day PC/laptops. For older children, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

The wireless network has an Encryption code this will help prevent hacking.

10. Monitoring

The e-Safety Leader and/or a senior member of staff should be monitoring the use of on-line technologies by children and young people and staff, on a regular basis. This will be carried out by the member of staff working with the children.

Network Managers/ICT technicians should not have overall control of network monitoring.

Teachers monitor the use of the Internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.

11. School library

The computers in the school library are protected in line with the school network. The same acceptable use rules apply for any staff and children and young people using this technology.

12. Parents

12.1 Roles

Each child or young person receives a copy of the Acceptable Use Rules on first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules. Children should be reminded of this policy regularly within school.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted. School keeps a record of the signed forms. The forms will be re-signed annually.

12.2 Support

We will inform Parents/Carers through appropriate means as and when necessary. If parents request any help we will direct them to use the Childnet International 'KnowITAll for Parents' on-line materials http://www.childnet.com/resources/know-it-all-for-parents) to deliver key messages and raise awareness for parents/carers and the community. A parent e-safety information session will be held by the e-safety leader annually to share relevant information.

The Appendices detail where parents/carers can go for further support beyond the school. The school will help to provide access to the Internet for parents/carers so that appropriate advice and information can be accessed where there may be no Internet at home, subject to arrangement.

13. Links to other policies

13.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour and discipline Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs.

13.2 Allegation Procedures and the Child Protection Policy

Please refer to the Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Headteacher immediately or Chair of Governors in the event of the allegation made about the Headteacher.

The DCFS White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people and young people about homework or any other school issues either in or beyond school and any such action should be dealt with.

We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.

Please refer to the Child Protection Policy for the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

13.3 PSHE

We link the teaching and learning of e-Safety with our PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people.

13.4 Health and Safety

Please refer to the Health and Safety guidelines and procedures for information on related topics, particularly Display Screen Equipment. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

13.5 School website

The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission is always sought from the parent/carer prior

to the uploading of any images. The school will consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

13.6 External websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

13.7 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Signed:_____

Date: November 2017

Date of review: November 2018

Appendix A

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the E2Bn who control the filtering service for school so that it can be added to the banned or restricted list.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Headteacher and e-Safety Leader immediately.
- Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the E2Bn filtering services as with A.

C. An adult receives inappropriate material.
- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website (or printed out) about an adult in school:
- Preserve any evidence.
- Inform the Headteacher immediately and follow Child Protection Policy as necessary.
- Inform the e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Appendix B

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
   - Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
   - Report website to the e-Safety Leader via teh e-safety incident log.
   - Contact the e2Bn helpdesk filtering service for school so that it can be added to the banned list or use Local Control to alter within your setting.
   - Check that filter levels are at the appropriate levels for staff and pupil use in school.

B. An inappropriate website is accessed deliberately:
   - Refer the child to the Acceptable Use Rules that were agreed.
   - Reinforce the knowledge that it is illegal to access certain images and police can be informed.
   - Report to the e-Safety Leader via the e-safety incident log.
   - Decide on appropriate sanction.
   - Notify the parent/carer.
   - Inform E2Bn as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
   - Ensure the child is reassured and remove them from the situation immediately.
   - Report to the Headteacher and Designated Person for Child Protection immediately.
   - Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
   - Report to the e-Safety Leader via the e-safety incident log.
   - If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy/Anti-bullying policy.
   - Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
   - Preserve any evidence.
   - Inform the Headteacher immediately.
   - Report to the e-Safety Leader via the e-safety incident log.
   - Inform the LA and e-Safety Leader so that new risks can be identified.
   - Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
   - Preserve any evidence.
   - Inform the Headteacher immediately.
   - Report to the e-Safety Leader via the e-safety incident log.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

- CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
- They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.
  If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board.

All adults should know who the Designated Person for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix C

Acceptable Use Rules for Staff

These rules apply to all use of digital media in school, on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

Use of equipment in school:

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I will protect myself by not using personal equipment in school or settings for work purposes, such as a digital camera or the use of a personal e-mail.
- I know I may take equipment home if it supports their work in school e.g: downloading files for work, support for planning, writing reports etc. but realise that is my responsibility to keep it in good condition.
- I have signed the Laptop agreement.
- I will ensure that any personal or confidential data is encrypted.
- I will not use memory sticks to store confidential information instead I will use school drives, or if I need to access information outside of school, I will use secure domains such as Google drive or Dropbox.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

Use of images:

- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I know that I should only store images of children on the shared drive at school and not on my laptop or personal computer.

Dealing with incidents:

- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know how and where to report incidents of misuse.

Use of technology:

- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I will only install hardware and software I have been given permission for.

- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and change it on a regular basis. I will not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed……. Date…….
Name (printed)…….
School……...

Appendix E

E-Safety Acceptable Use Rules Letter to Parents/Carers

GROWING, LEARNING, ACHIEVING TOGETHER
Highland Close, Bletchley, Milton Keynes, MK3 7PD. Telephone: (01908) 270377 Fax: (01908) 375562
Headteacher: Louise Aird B.A., P.G.C.E, N.P.Q.H,
ColdHarbour@milton-keynes.gov.uk

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet, E-mail and other technologies. In order to support the school in educating your child about e-Safety (safe use of the Internet), please read the following rules with your child/young person then sign and return the slip. In the event of a breach of the rules by any child or young person, the e-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home). This will all help to keep your child safe.

Additional information can be found on the 'Know IT all' website, https://www.thinkuknow.co.uk/parents/ .

Should you wish to discuss the matter further please contact your child's class teacher, myself or the school office.

Yours faithfully,

Miss Ruth Burgess

E-Safety Acceptable Use Rules Return Slip

Name of child:_____Class:_____

Child Agreement:

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.
- I will work with my child so that we can set up rules for going online. Such the time of day that they can be online, the length of time they can be online, and areas they are allowed to visit.
- I will set up safety mechanisms to safeguard my child/ren on the internet and know I can seek the schools support and use http://www.vodafone.com/content/parents.html if I am unsure how to do this.

Parent/Carer Signature: _____ Date: _____

From time to time we may like to put your child's photograph up on Class Dojo to celebrate the work they have been doing in class. Class Dojo is only viewable to Parents at Cold Harbour School and is not publicly accessible. Should we want to use your child's photo in a more public domain such as our website or Facebook page we will contact you separately. Please indicate below if you are happy for us to do this.

I do/do not (delete as applicable) give permission for my child's photograph to be shown on Class Dojo.

Parent/Carer Signature: _____ Date: _____

Appendix F

AUP - EYFS and Key Stage 1 (years 1 and 2)

These are our rules for using the Internet safely.

Our Internet and E-mail Rules

- We use the Internet safely to help us learn.
- We learn how to use the Internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name, or we use a 'made-up' name.
- We don't tell people on the internet any other information about ourselves, especially where we live or the school we go to.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we use 'Hector Protector' to cover it up, close our screen or turn off the monitor and tell an adult straight away.
- We know that it is important to follow the rules.
- We are able to look after each other by using our safe Internet.
- We can go to www.thinkuknow.co.uk for help.

Appendix G

AUP - Key Stage 2 (Years 3-6)

These are our rules for using the Internet safely and responsibly.

Our On-line Rules
• We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly. • We send e-mails and messages that are polite and friendly. • We will only e-mail, chat to or video-conference people an adult has approved and is present to monitor us. • Adults are present when we use on-line tools, such as video-conferencing. • We know how to use safe search engines (Swiggle) or to set filters in Google to their highest settings. • We never give out passwords or personal information (like our surname, address or phone number). • We never post photographs or video clips without permission and never include names with photographs. • If we need help we know who to ask. • If we see anything on the Internet or in an e-mail that makes us uncomfortable, we know what to do. • If we receive a message sent by someone we don't know we don't open it but tell an adult instead. • We never agree to get together with someone I "meet" online without first checking with my parents/carers. If my parents/carers agree to the meeting, I will be sure that it is in a public place and bring my mother, father or carer along. • We know we should follow the rules as part of the agreement with our parent/carer. • We are able to look after each other by using our safe Internet in a responsible way. • We know that we can go to www.thinkuknow.co.uk for help.

Appendix H

Further Information and Guidance

The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- http://ceop.police.uk/ (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 7)
- www.phonebrain.org.uk (for Yr 5 – 8, safe mobile phone usage)
- www.dcsf.gov.uk (for adults)
- http://www.mkscb.org/mkscb/ (Local Safeguarding Children's Board Milton Keynes – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)
- http://www.kidsmart.org.uk/teachers/ (SMART adventure resources)
- http://www.childnet.com/resources (Wide range of resources)
- http://www.net-aware.org.uk/# (Reviews apps and websites suitable for children. Updated regularly to account for current trends)