E-SAFETY AND ACCEPTABLE USE OF IT POLICY, INCLUDING DATA SECURITY AND MANAGEMENT

Information and Communications Technology (ICT) is a resource to support learning as well as playing a role in the everyday lives of children; and as such they need to learn the skills to safely access life-long learning. ICT covers a wide range of resources including web-based and mobile learning, and it is also important to recognise the constant change of ICT within society. Currently the internet technologies children are able to access include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst potentially exciting and beneficial both in and out of the classroom, much ICT, particularly web-based resources, are not consistently policed. Therefore all users need to be aware of the range of risks associated with the use of these technologies and that some have minimum age requirements, usually 13 years.

We have a responsibility to educate the children on E-Safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, both in and beyond the context of the classroom.

In addition schools hold personal data on children, staff and others to conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information is unacceptable due to the potential dangers and this can make it difficult for the school to use technology to benefit learners. Therefore everyone in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. (Please see our Data Protection Policy.)

Roles and Responsibilities:

The Head Teacher and Governors have ultimate responsibility to ensure that there is a robust policy and practices to ensure E-Safety. The IT manager oversees E-Safety and staff training; and all members of the school community are aware of this.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. All staff and children sign the acceptable use agreement.

Parental Involvement:

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school or if the agreement is updated.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website).
- The school disseminates information to parents relating to E-Safety where appropriate in the form of:
    - Information evenings
    - Practical training sessions
    - Newsletter items

E-Safety in the Curriculum:

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

- The school provides opportunities to learn about E-Safety.
- Educating children about the online risks that they may encounter outside school is done both formally as part of the curriculum and informally when opportunities arise.
- Children are made aware of the relevant legislation when using the internet, such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Children are taught about copyright, respecting other people's information and protecting their own personal information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Children are aware of the impact of Cyber-bullying and know how to seek help if they are affected by any form of online bullying. They 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 Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the IT curriculum.
- The school endeavours to create a consistent message with parents for all children. Staff are aware that some pupils may require additional support or 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 and young people.

E-Mail:

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to be prepared for secondary school pupils must have experienced sending and receiving e-mails.

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. All staff follow the Data Protection Policy.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Children may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows: delete all e-mails of short-term value; organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- Children have their own individual school issued accounts within our VLE which the children use for electronic communication.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments. E-mails must not be used by any member of the school community to send or receive indecent or offensive images, videos or

any written material of this kind. In addition, e-mails should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.
- Children must immediately tell a teacher/trusted adult if they receive an offensive e-mail whether directed at themselves or others and before it is deleted.
- Staff must inform the IT manager or Head Teacher if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.
- Children are introduced to e-mail as part of the ICT Scheme of Work.
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail practices apply.
- E-mails created on the school system are considered to be the property of the school.

Sending E-Mails:
- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily.
- School e-mail is not to be used for personal advertising.

Receiving E-Mails:
- Check your e-mail regularly, and note our Communication Commitment.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult the IT manager or technician first if in doubt.
- The automatic forwarding and deletion of e-mails is not allowed.

E-Safety Support for Staff:
- Our staff receive regular and appropriate information and training on E-Safety and how they can promote the 'Stay Safe' online messages.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their 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.
- All staff are incorporate E-Safety activities and awareness within their teaching.

The Internet:

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.
- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with children.
- 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 observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- On-line gambling or gaming is not allowed.
- School internet access is controlled through EXA's web filtering service.
- The Senior Leadership Team is aware of its responsibility when monitoring staff communication under current legislation.
- Staff and children are aware that school based e-mail 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 children discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and IT manager as appropriate.
- It is the responsibility of the school to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Children and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the IT manager.
- If there are any issues related to viruses or anti-virus software, the IT manager should be informed.
- The school does not allow any access to social networking sites.

We believe that it is essential for parents/carers to be fully involved with promoting E-Safety and to be aware of their responsibilities. We consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Images and film:

Taking of Images and Film:

Digital images are easy to capture, reproduce and publish and, therefore, misuse. Written consent of parents and staff is required for staff and pupils to take appropriate images with school equipment.

- Staff and visitors are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including field trips. Appropriate images can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted from the individual device. If a school device is unavailable then the situation should be discussed with the Head Teacher.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Head Teacher.
- Staff must have permission from the Head Teacher before any image can be uploaded for publication beyond the VLE.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.
- Where an outside company or individual is commissioned by the school to take images, there is appropriate DBS clearance in place and the school is satisfied that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.
- Storage of images which attach addresses/location of images on the file is not permitted.

Publishing Children's Images and Work:

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos. A list of parents who have not given permission can be found in the office. This consent form is considered valid for the entire period that the child attends the 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 or carers may withdraw permission, in writing, at any time. Children's names will not be published alongside their image and vice versa. E-mail and postal addresses of children will not be published. Children's full names will not be published. Before posting a child's work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images:

- Images/ films of children are stored on the school's network.
- E-storage of images on personal portable media e.g. USB sticks by pupils or staff is not permitted without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

Web Cams and CCTV:

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the school community will result in sanctions. Staff must ensure web cams are switched off when not in use.

Video Conferencing:

- Permission is sought from parents and carers if their children are to be involved in a video conference.
- All children are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the IT manager 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.

Personal Mobile Devices (including phones):

- The school allows staff to bring in personal mobile phones and devices for their own use. The school only allows a member of staff to contact a pupil or parent/carer using their personal device in emergencies when no other form of communication is available.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages, images (including pseudo images), videos or sounds between any members of the school community is not allowed.
- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Security:

All personal data is stored securely and is managed in accordance with the relevant legislation. The school gives relevant staff access to its Management Information System, with a unique username and password

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others. Passwords should be secure and will be set to change periodically.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.
- All ICT equipment is security marked as soon as possible after it is received. The office maintains a register of all ICT equipment and other portable assets.
- As a user of the school ICT equipment, staff are responsible for their own activities.
- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's equipment register.
- It is imperative that staff save their data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any of their data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is necessary to do so the local drive must be

encrypted.
- A time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network without the permission of the IT manager.
- On termination of employment, resignation or transfer, staff must return all ICT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- The installation of any applications or software packages must be authorised by the IT manager.
- Portable equipment must be transported in its protective bag.

Server Security:
- School servers are kept in a locked and secure environment and there are limited access rights to these which are password protected.
- Existing servers should have security software installed appropriate to the machine's specification and the school uses a remote back up service and data is backed up daily.

Using Removable Media:
- Always consider if an alternative solution already exists.
- Only use school provided removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by the IT support team.
- Use of private cloud storage is not permitted.

Monitoring:

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

Internet activity is logged by the school's internet provider and in addition the support technician regularly monitors the web sites which are accessed on school equipment.

Breaches:

A breach or suspected breach of policy by a school employee, contractor or child may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting:

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's IT manager. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

An incident log is used to monitor what is happening and identify trends or specific concerns. The log is kept by the ICT manager.

- 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 IT manager. Depending on the seriousness of the offence investigation by the Head Teacher will follow; possibly leading to disciplinary action, dismissal and involvement of Police for very serious offences.

Personal, Sensitive, Confidential and Classified Information:

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access.
- Personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- The security of any personal, sensitive, confidential and classified information contained in documents which are faxed, copied, scanned or printed.
- Only download personal data from systems if expressly authorised to do so by the Head Teacher.
- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
- Hard copies of data are securely stored and disposed of after use in accordance with the document labeling.
- They protect school information and data at all times, including any printed material.

Viruses:

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Interference with any anti-virus software installed on school ICT equipment is not permitted.
- Any machine not routinely connected to the school network, must have a virus update run by the IT manager before use.
- If there is any suspicion that there may be a virus on any school ICT equipment, the equipment must not be used until checked.

Disposal of ICT Equipment:

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. Disposal of any ICT equipment will conform to current legislation.

Zombie Accounts:

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. Therefore our technical support staff will ensure that all user accounts are disabled once the member of the school has left the school.

Cheddington Combined School

Acceptable ICT Use Statement - Staff

The computer system is owned by the school and is made available to children to further their education and to staff to engage their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties: the children, the staff and the school.

The school takes active steps to filter inappropriate sites on equipment while on school premises and actively monitors the use of computer equipment both in and out of school.

Staff with internet access should sign a copy of this statement and return it to the IT manager.

- Access to school ICT systems should only be made via an authorised account and password. This should not be made available to any person outside the school, unless specifically permitted by the IT manager.
- All activity using ICT systems in school time (7am to 5pm) should be appropriate to staff professional activity or student's education.
- Personal use of staff laptops at home is acceptable. However, it is expected that staff do not use communication technology in ways which might compromise their code of professional conduct either in or out of school. (For example: posting derogatory or otherwise inappropriate content onto sites to which pupils or parents might have access, sending anonymous messages, etc)
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is not acceptable. (For example: deliberately spreading viruses or downloading software without taking reasonable precautions to ensure that it will not cause compatibility problems.)
- Copyright of materials must be respected and staff should take care to ensure the security and integrity of any data under their care. (For example: Information which could lead to the identification of a pupil's name and address should not be held on memory sticks which might easily be lost.)
- Communication by e-mail, or other electronic media must have the same professional levels of language and content which would be applied to postal letters or other written communications from school.
- Use of school ICT equipment to access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden.

Please note that details of what constitutes professional conduct are set out by, and available from, the General Teaching Council.

Full name:

Signed: Date:

This is Bucks County Council generic Code of Practice for Schools. It is parent/guardian's responsibility to ensure that children understand the important points and what is and is not acceptable when using the internet. Further guidance will be given to individual classes by staff before each session that requires use of the internet.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If any child violates these provisions, access to the Internet will be denied and the child will be subject to disciplinary action.

Additional action may be taken by the school in line with existing policy regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Children's Internet Code of Practice:

- I will only use the internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- I will never send anyone my picture without permission from my teacher/parents/carer.
- I will never give my password to anyone, even my best friend and I will log off when I have finished using the computer.
- I will never arrange to meet anyone in person without first agreeing it with my parents/teacher/carer and get them to come along to the first meeting.
- I will never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report it to a teacher or parent.
- I will never respond to unpleasant, suggestive or bullying e-mails or bulletin boards and I will always report it to a teacher or parent.
- I will not look for bad language or distasteful images while I'm online and I will report bad language or distasteful images to a teacher or parent if I come across them accidentally.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I know that my teacher and the Internet service provider will check the sites I have visited!
- I understand that I can access only sites and material relevant to my work in school and that I will not be able to use the Internet if I deliberately look at unsuitable material.
- I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I know that the contents of my e-mail messages will be monitored by the Network Manager.
- I may not download software from the Internet (including screen savers, games, video clips, audio clips, *.exe files).
- I know that information on the Internet may not always be reliable and sources may need checking. Web sites may be sponsored by advertisers.
- I will not use e-mail to send or encourage material which is illegal, offensive or annoying or invades another person's privacy

Child's Name.....….. School ……

I have read the Children's Code of Practice and I have discussed it with my son/daughter/ward. We agree to support the school's policy on the use of the Internet.

Signed (Parent/Guardian/Carer) ……Pupil ……..……Date ……..

Policy reviewed: Summer 2019

Date of next review: Spring 2020