ICT Usage and E-Safety Policy

Learning at Charville is underpinned by our Core Values, which are as follows:

Respect
Independence
Self-belief
Honesty
Caring
Determination

1. Scope

This policy applies to school based employees who are directly employed by the school. It applies to all users of the School's network, and the use of the school's computer facilities, (including telephony, hardware, software, e-mail, internet, etc) used anywhere, for professional or personal purposes whether in working time or in the employee's own time.

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 as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook (school page) 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 exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Charville 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.

Schools hold personal data on learners, staff and other people to help them 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 can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody 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 will be made aware of the risks and threats and how to minimise them.
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, 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).

2. Purpose

The purpose of this policy is to:

- Protect employees by making clear what is acceptable use of the school's computer facilities.

- Protect the security and integrity of the school and its computer facilities.

- To outline education to 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.

3. Policy

High standards of conduct and probity are as relevant to the use of the school computer facilities as they are to all other aspects of work, and employees must conduct themselves in line with the school's code of conduct and disciplinary code.

Employees who are in any doubt about what is, or is not, acceptable use of the school's computer facilities must seek advice from their manager or the designated ICT person in advance of the use.

Employees must conduct themselves honestly, appropriately and in accordance with the law and this policy when using the school's computer facilities.

Breach of this policy may lead to disciplinary action and result in withdrawal of access to some or all computer facilities. Serious breaches may be regarded as gross misconduct and may lead to dismissal. Employees and Governors are required to sign a statement agreeing to the terms and conditions of this Policy (Appendix 1).

The school will co-operate with any law enforcement activity.

Managers must ensure that employees have the skills to use the school's computer facilities.

The school will purchase all hardware and software through approved suppliers.

4. Access

The school provides access to ICT to enable employees to undertake their duties.

The Head Teacher or another designated senior person has authority to obtain access to an employee's data and documents.

5. Monitoring

Each employee will be required to sign the Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy.

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business

related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Each employee will be required to sign the Statement of Acceptance of the Terms and Conditions of the ICT Usage Policy.
The school's computer facilities will be monitored to ensure this policy is adhered to and that these facilities are used properly.

Any information (including personal emails, documents, etc) within the school's network or equipment can be inspected, at any time, without notice.

6. Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil 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.

7. Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT in school must be immediately reported to the Head Teacher or Deputy Head Teacher.

8. Personal use

Employees can use the school's computer facilities for reasonable personal use provided it:

- Does not interfere with the performance of their duties;
- Is appropriate;
- Is on an occasional, rather than a regular or substantial basis;
- Does not compromise the security of the school's systems or reputation.

9. e-Safety - Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is the Head Teacher who has been designated 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.

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

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety,

home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

10. e-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. 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 staff continually look for new opportunities to promote e-Safety.

The school has a framework for teaching internet skills in Computing/SMSC lessons
The school provides opportunities within a range of curriculum areas to teach about e-Safety, including Staying Safe week

Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum

Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. 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/ or trusted staff member

All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas managing the School Safety Messages

Staff aim to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used

11. Smile and Stay Safe Poster

e-Safety guidelines to be displayed throughout the school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

12. E-Mail

The use of e-mail within most schools is an essential means of communication for both staff. In the context of school, e-mail should not be considered private. Educationally, e-

mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. Staff recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

Managing e-Mail

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

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

Staff must inform the Head Teacher or Deputy Head Teacher if they receive an offensive e-mail

Pupils are introduced to e-mail as part of the Computing Scheme of Work

However school e-mails are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

13. Sending e-Mails

When sending emails staff should:

- Remember that If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section
- E-mailing Personal, Sensitive, Confidential or Classified **Information**
- Use own school e-mail account or the Charville email account (if you have assigned rights) so that member of staff is 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
- Remember that school e-mail is not to be used for personal advertising
- Use pupils initials as opposed to pupil names in their emails for child protection purposes.

14. Receiving e-Mails

When receiving emails staff are expected to:

- Check e-mails regularly, to never open attachments from an untrusted source and to consult their network manager first
- Not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- Remember that the automatic forwarding and deletion of e-mails is not allowed

15. E-mailing Personal, Sensitive, Confidential or Classified Information

Where the conclusion is that e-mail must be used to transmit such data, staff should:

- Obtain express consent from your manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail

- Encrypt and password protect http://www.thegrid.org.uk/info/dataprotection/#securedata. STAFF TO BE NOTIFIED
- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information where there are any concerns about the individual/s
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any body/ person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

16. Inappropriate Use

Employees must not use the school's computer facilities to:

- Send or access messages that are, or perceived to be, libellous, harassing or defamatory, or cause offence to the dignity of an individual or group.
- Access inappropriate internet sites or material. These may include pornographic, racist or any other sites not appropriate for a school. In the case of accidental access, the employee must immediately disconnect and inform their manager.
- Store, view, print or redistribute any inappropriate material.
- Access chat rooms, social networking sites or newsgroups for personal use.
- Advertise or send personal messages to large groups internally or externally unless through a specified facility or with the permission of an authorised person.
- Spread harmful programmes that may damage the school's computer facilities.
- Download, use or distribute software including entertainment software or games.
- Download video and audio streaming for personal purposes.
- Use their school e-mail address for the purchase of personal goods or financial transactions.

17. Safe Use of Images

Digital images are easy to capture, reproduce and publish and, therefore, misuse. Employees 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

Parents and carers are not permitted to take pictures or videos during school plays, productions and assemblies

Employees are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Head Teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device

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

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Managed Learning Environment

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

Images and videos are not permitted to be shared on any social network by staff or parents.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Images/ films of children are stored on the school's network

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

18. Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the site manager. The Head Teacher and Deputy Head Teacher. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx

Publicly accessible webcams are not available in school

Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults

Staff must ensure webcams are pushed into the closed position at all times on school computers and not left open at any time

Misuse of the webcam by any member of the school community will result in sanctions

Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

For further information relating to webcams and CCTV, please see http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml

19. School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment , you are responsible for your activity
- ICT equipment must be signed out, returned, charged and signed back in to the ICT cupboard
- Staff are made aware that ICT equipment is their responsibility if signed out to use in class
- Staff must ensure that their classroom is locked if leaving ICT equipment unattended

- Charville logs ICT equipment issued to staff and records serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school network. You are responsible for the backup and restoration of any of your 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 device. If it is necessary to do so the local drive must be encrypted
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager.

Authorising Managers are responsible for:

- maintaining control of the allocation and transfer within their Unit
- recovering and returning equipment when no longer needed

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section on the HGfL
http://www.thegrid.org.uk/info/dataprotection/

- Only use recommended removable media
- Encrypt and password protect – See P 14
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

20. Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- 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
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

21. Mobile Technologies

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device
- Pupils in Year 6 are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within school.
- At all times the device must be switched onto silent
- The school is not responsible for the loss, damage or theft of any personal mobile device
- 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 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 (including phones)

- 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 iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

22. Confidentiality and Security of Data

The school is legally responsible for all information stored or transmitted by its computer systems and for any improper disclosure. Disclosure of data, even unintentionally, can breach the Data Protection Act. Security measures are in place to ensure the confidentiality of data held by the school and employees are accountable for breaches of security or confidentiality.

- Employees must not attempt to disable or evade any security facility.
- User IDs and passwords must be kept secure and confidential, and passwords changed if an unauthorised person may be aware of them.
- Employees must carefully address e-mails to avoid sending sensitive information to the wrong recipient.
- Employees must ensure that data they are storing, updating or transmitting is accurate, and must not amend or alter e-mails they receive.
- To ensure security it may be necessary to prevent machines with sensitive data from connecting to the internet, or restrict usage of file transfers.

- Employees must use the appropriate system/method e.g., password-protected screen saver, if leaving their computer for short periods and switch computers off at the end of the working day
- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- If employees are aware of a breach of security with their password or account inform the Head Teacher or Deputy Head Teacher immediately

23. Copyright, Legal and Contractual Issues

Downloading and copying data and software or sending the work of others to third parties without permission can infringe copyright. The school retains the copyright to any original ICT based material produced by an employee in the course of their duties.

- Copyright should be checked and appropriate permissions sought. In the case of subscription services the appropriate licenses must be obtained.
- Software can only be downloaded with permission from the Head Teacher or the designated authorised ICT person. Downloaded software becomes the school's property and must be used only under the terms of its license. Employees must arrange to license and register such software, where required. Software downloaded without permission must be deleted.
- Employees must not transfer any software licensed to the school or data owned or licensed by the school without authorisation from the Head Teacher or the designated ICT person.
- The use of computer facilities can lead to contractual obligations in the same way as verbal or written transactions. Employees must not exceed their delegated authority to enter into contracts or authorise expenditure.
- Records of computer transactions must take place through archiving or backup. Where appropriate, confirmation of receipt of important e-mails must be gained which may be disclosed in litigation.
- Transactions through computer facilities must be treated in the same way as transactions on the school's headed paper.

24. Network Efficiency

Employees must regularly delete or archive files no longer required or needed for immediate access.

All files will be scanned for viruses.

Wherever possible intensive operations such as large file transfers, video downloads, mass e-mailing should be scheduled during off-peak hours.

Video and audio streaming and downloading must be for work purposes only.

25. Computer 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

Never interfere with any anti-virus software installed on school ICT equipment that you use

If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know

26. Software

The school must ensure all software is legally licensed and is responsible for managing and maintaining the register of software and for holding licenses and the original media.

- No software can be loaded onto or used on any computer owned or leased unless approved by and licensed to the school.
- All software must be procured by the school and installed by the designated authorised ICT person.
- Software must not be copied or distributed by any means without prior approval from the Head Teacher or the designated authorised ICT person.

27. Telephone Services

- Staff are responsible for the security of their school mobile phone.
- A PIN code must always be set on your school mobile phone and not left unattended or on display (especially in vehicles)
- Staff must read and understand the user instructions and safety points relating to the use of their school mobile phone prior to using it
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default

28. Social Media, including Facebook and Twitter

Charville uses Facebook to communicate with parents and carers.

- The Head teacher and Deputy Head teacher are responsible for all postings on these technologies and on Facebook, monitors responses from others
- Staff are not permitted to access their personal social media accounts using school equipment at any time during the school day.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

29. Authority to Express Views

Employees using school computer facilities must communicate the school's, and not their personal, views.

Employees must not participate in newsgroups/chat rooms/social networking sites, unless in a professional capacity relevant to their duties and with prior agreement from their manager or the designated authorised person.

Employees must not use the school or its name to endorse any non school commercial product or service.

30. Parental Involvement

Charville believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. Staff regularly 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.

The school disseminates information to parents relating to e-Safety where appropriate in the form of;

- Information and celebration evenings
- Practical training sessions e.g. How to adjust the Facebook privacy settings
- Posters
- School website
- Newsletter items
- MLE
- Letters
- Text Messages
- Social Media, e.g. Facebook page

31. Acceptable Use Agreement: Pupils - Primary

Charville Primary Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords (except my parents).
- I will only open/ delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using ICT in school because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT in school can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- I understand that my access to ICT equipment in school can be taken away if I am found to be misusing the equipment and breaking the E-Safety rules.

32. Acceptable Use Agreement: Staff, Governors and Visitors

Staff and Governor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, 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 in school. All staff are expected to sign this policy and adhere at all times to its contents when using school ICT equipment on site or off site. Any concerns or clarification should be discussed with the Head Teacher/ Deputy Head Teacher.

- I will only use the school's email / Internet / Internal online systems / Learning Platform 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, including social networking, are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) 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 Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Head Teacher/ Deputy Head Teacher.
- I will not browse, download, upload or distribute any material in school that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line 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 Head Teacher.
- All images of children must only be taken using school cameras.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies in school can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.
- 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 and Data Security policies 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 and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..…… (printed)

Job title . . . . . .

33. Writing and Reviewing this Policy

Review Procedure

- There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue that concerns them
- There will be on-going opportunities for staff to discuss this policy with the Head Teacher and ICT coordinator
- This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Approved by Governing Body: Spring 2015
Review date: Spring 2016

34. Current Legislation

Acts Relating to Monitoring of Staff email
Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)
(Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006
It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or

persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

access to computer files or software without permission (for example using another persons password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud)

impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
The Freedom of Information Act 200
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx