RED HOUSE SCHOOL

E-SAFETY POLICY

INTRODUCTION

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

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society 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 (but not exclusive to) Facebook, Twitter, Snapchat & Instagram
- smart phones
- other mobile devices with web functionality
- gaming, especially online
- learning platforms and VLE (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, is 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 Red House School 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 the 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 should 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).

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 designated teacher for Child Protection (Safeguarding) is Danny Kitching. The e-Safety Coordinators are Lucy Waldock (Junior School) and Graeme Butterfield (Senior School). The e-Safety Coordinators report to the designated teacher. All members of the school community have been made aware of who holds these posts. It is the role of the e-Safety Coordinators to keep abreast of current issues and guidance through organisations such as SLSCB (Stockton Local Safeguarding Children Board), CEOP (Child Exploitation and On-line Protection) and Childnet.

Senior Management and governors are updated by the Head/e-Safety Coordinators 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 & safety, behaviour management, anti-bullying and PSHE.

MONITORING

The Network Manager may inspect any ICT equipment owned or leased by the school at any time without prior notice.

The Network Manager 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 Red House staff 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.

The Network Manager may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by the Network Manager and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

EYFS, Key Stages 1-2
Acceptable Use Agreement/e-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school e-mail address when e-mailing in school.
- 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.
- 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 not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT 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 can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.

Senior School Pupils – Key Stages 3-4
Acceptable Use Agreement/e-Safety Rules

Security and Privacy

• I will not disclose my password to others, or use passwords intended for the use of others.
• I will not use the computers in a way that harasses, harms, offends or insults others.
• I will not attempt to bypass, security in place on the computers, or attempt to alter the settings.
• I will not download programs from the Internet nor have executable files in my network storage area.

Internet

• I will not access the Internet unless for study or for school authorised/supervised activities.
• I will not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
• I will respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
• I will not engage in 'chat' activities over the Internet.
• I will use my school Office 365 account for study or for school authorised activities only.

Electronic Devices

• I will use school ipads, or other electronic devices brought from home, such as smartphones, for educational purposes only. This includes the taking of pictures, and communications using these devices.

A breach of the above will act as a failure to comply with the School's Acceptable Use Policy relating to the use of ICT facilities and electronic devices in school, and disciplinary action will be taken.

Staff, Governor and Visitor
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. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Lucy Waldock (Junior School) or Mr Graeme Butterfield (Senior School), the School's e-Safety Coordinators or the Head.

- I will use the school's email/internet/intranet/learning platform and any related technologies for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will not accept as friends current pupils on a personal social network site.
- 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. I will not install any hardware of software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes 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.
- I will not use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless using school owned storage devices, e.g. SD cards, or with the permission of the Head.
- 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 can be monitored and logged and can be made available, on request, to my Line Manager or Head.
- 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 Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

ACCEPTABLE USE AGREEMENT/e-SAFETY RULES PROCEDURES

A copy of the acceptable use agreement/e-Safety rules will be sent to parents each year. Class teachers and tutors will also discuss the AUA with pupils each year.

As part of the induction process all new staff, or governors and visitors who have been provided with access to the schools network, will be issued with the acceptable use agreement/code of conduct which they will be expected to sign. A copy of this will be kept within staff files.

BREACHES OF e-SAFETY POLICY

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. Policy breaches may also lead to criminal or civil proceedings.

The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.
The data protection powers of the Information Commissioner's Office are to:

- conduct assessments to check organisations are complying with the Act
- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period
- serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- prosecute those who commit criminal offences under the Act;
- conduct audits to assess whether organisations processing of personal data follows good practice,

- report to Parliament on data protection issues of concern

STAFF PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the internet, in school and outside school, for your own protection we advise that you:

- ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately
- only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SMT.
- do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.
- you have a duty to report any e-Safety incident which may impact.

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

e-MAIL

The use of e-mail within schools is an essential means of communication for both staff and pupils. 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. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'.

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.
- 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.
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of Red House School'.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under 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 by organising e-mail into folders and carry out frequent house-keeping on all folders and archives.
- Pupils have their own individual school issued accounts from Years 2-11.
- Staff must inform (the e-Safety Co-ordinator/line manager) if they receive an offensive e-mail.
- Pupils 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 policies apply.
- Check your e-mail regularly, i.e. daily during term time.
- If appropriate to your role, activate your 'out-of-office' notification when away for extended periods.

- Never open attachments from an untrusted source; consult the Network Manager first.

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 e-Safety.
- The school has a framework for teaching internet skills in ICT lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils about the online risks that they may encounter outside school is done when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- 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/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.
- Our staff receive regular information and training on e-Safety.
- 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 encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-Safety policy will be introduced by class teachers or form tutors to the pupils at the start of each school year.
- E-Safety posters will be prominently displayed.

INTERNET ACCESS

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. Whenever any inappropriate use of the internet is detected it will be followed up.

Managing the Internet

- 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 pupils
- 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 check these sites the children are using 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

Infrastructure

- The School's internet access is controlled and monitored through the School's web filtering service. For further information relating to filtering please consult the Network Manager.
- Red House School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further, if required
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download Apps, programs or files on school based technologies without seeking prior permission from the Network Manager.

- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed.

INCIDENT REPORTING, e-SAFETY INCIDENT LOG AND INFRINGEMENTS

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected serious misuse of ICT must be immediately reported to your line manager.

Misuse and Infringements

Complaints

Complaints and/or issues relating to e-Safety should be made to the e-Safety Coordinator or Head.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Coordinator.
- Deliberate access to inappropriate materials by any user will be reported to the e-Safety Coordinator. Serious offences will be dealt with through the Behaviour Management Policy (pupils) or Discipline and Poor Performance Policy (staff).

MANAGING WEB TECHNOLOGIES

- Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.
- Pupils are not permitted to access social networking websites. On-line games websites may only be used by pupils within school when authorized by a member of staff.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Cyberbullying is not tolerated at Red House. Any instances of cyberbullying must be reported to a teacher.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Head.

PARENTAL INVOLVEMENT

- We 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. We regularly consult with parents/carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.
- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy through discussion within Pupil Council and by School Council.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- 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.
- The school disseminates information to parents relating to eSafety where appropriate in the form of:
  - information and celebration evenings
  - practical training sessions
  - posters
  - school website
  - newsletter items
  - information leaflet 'Red House ICT and e-Safety'

PASSWORDS AND PASSWORD SECURITY

Passwords

- Always use your own personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.

- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to the Network Manager when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you are aware of a breach of security with your password or account inform the Network Manager immediately.

It is advised that:
- 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.
- User ID and passwords for staff and pupils who have left the school are removed from the system within 24 hours.

If you think your password may have been compromised or someone else has become aware of your password report this to the Network Manager.

Password Security
- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.
- Users are provided with an individual network, email, learning platform and Management Information System (where appropriate) log-in username. They are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers or teachers. On-line materials held in shared areas or on the i-drive are accessible.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Computers attached to the school's internet are automatically locked after 15 minutes of inactivity.

SAFE USE OF IMAGES AND FILM

Taking of Images and Film
- 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
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils unless using school owned storage devices, e.g. SD cards. This includes when on educational visits. However with the express permission of the Head, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Head.
- Pupils and staff must have permission from the Head before any image can be uploaded for publication

Consent of Adults Who Work at the School
Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

Publishing Pupil's Images and Work
- On a child's entry to the school, all parents/carers, as part of the Parental Contract, are asked to give permission to use their child's photos or images.
- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.
- has been given for work to be displayed.
- Only the Head of Marketing or Head's PA have authority to upload to the website.

Storage of Images
- Images/films of children are stored on the school's network and secure cloud-based server.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Head.
- 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
- Staff have the responsibility of deleting the images when they are no longer required.

Webcams and Closed Circuit Television (CCTV)

- The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.
- 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 (as listed under the 'inappropriate materials' section of this document).

Further information on the use of CCTV can be found in the Policies & Procedures document.

Video Conferencing and Remote Lessons

The school uses Microsoft Teams for virtual meetings and lessons. This is covered by the Remote Teaching & Learning Guidelines.

SCHOOL ICT EQUIPMENT INCLUDING PORTABLE AND MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity.
- ICT equipment issued to staff is logged by the Network Manager and a central record of serial numbers is kept as part of the school's inventory.
- Visitors may not plug their ICT hardware into the school network points (unless special provision has been made by the Network Manager). 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
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- On termination of employment, resignation or transfer, return all ICT equipment to the Network 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 redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable and 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

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, Blackberries, iPads, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

BRING YOUR OWN DEVICE (BYOD)

The School recognises that as technology has changed more pupils have access to Internet capable devices. This should be seen as a resource and provide an opportunity to enable quick and easy access to the Internet to enhance learning. Devices in the form of mobile phones, music players and tablet computers should no longer be looked on as distractions or contraband but should be used in classrooms to aid learning when short bursts of activity are required and a mobile device is more appropriate than a laptop or desktop computer.

General Information

Access to the Red House School wireless network, whether with school-provided or personal devices, is filtered in compliance with the Children's Internet Protection Act (CIPA). Pupils will not have access to any documents which reside on the school network from their personal devices.

Access to the Red House School wireless network is a privilege, not a right. Any use of the wireless network entails personal responsibility and compliance with all school rules. The use of the network also allows IT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request.

Obtaining Access to the Network

To obtain access to the network staff or pupils will need to provide the IT Network Manager with the MAC address of their device enabling them to be given the access key. This can be done in an individual email or by the class teacher making a list of pupils and emailing it to the Network Manager. If pupils or staff are not sure how to find the MAC address then the IT Manager can help.

If a teacher asks a class to use their mobile device and pupils do not already have access to the network, the wireless access key can be provided enabling them to use their device. The IT Network Manager should be emailed the MAC address of the device(s) that have been allowed to access the network as soon as possible following the lesson/activity.

Guidelines for Use

- Use of personal devices during the school day is at the discretion of teachers and staff. Pupils must use devices as directed by their teacher.
  The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. gaming, gambling or accessing social network sites is not allowed within school and contacting parents, should only take place after permission has been given from a teacher or other member of staff.
- The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.
- The use of personal devices falls under Red House School's Acceptable Use Policy, found in the student handbook.
- Pupils shall not use personal devices outside of their classroom, e.g. break and lunchtimes, unless otherwise directed by their teacher e.g. on school visits or activities.
- Pupils shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
- Pupils shall not create, store or distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

Consequences for Misuse/Disruption

(one or more may apply):

- access to the wireless network will be removed.
- device taken away for the period.
- device taken away and kept in the front office until parent picks it up.
- pupil is not allowed to use personal devices at school.
- Serious misuse of Internet or other mobile technology capable devices is regarded as a serious offence within the School's Behaviour Management and Disciplinary Policies and will be dealt with in accordance with these policies. The police will be advised where inappropriate or illegal content or activity is suspected, reported or identified.

School Liability Statement

Pupils bring their devices to use at Red House School at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

Red House School is in no way responsible for:

- personal devices that are broken while at school or during school-sponsored activities.
- personal devices that are lost or stolen at school or during school-sponsored activities.
- maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

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 are allowed to bring personal mobile devices/phones to school but they must be switched off during the school day unless otherwise directed by staff.
- This technology may be used for educational purposes (see BOYD). The device user, in this instance, must always ask the prior permission of the bill payer.
- 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.
- The school is aware that many pupils can access the internet through 3G/4G connections. Staff will be vigilant to try and minimize access to inappropriate material though the pupils' personal connections.

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

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

SOCIAL MEDIA including Facebook and Twitter

- Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.
- Our school uses Facebook and Twitter to communicate with parents and carers. The Head of Marketing is 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 during school hours.
- Staff are able to setup social media accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Facebook or other applications.
- Staff may, with the Head's permission, set up departmental social media accounts to promote the School. Staff may interact with School social media accounts i.e. liking on Facebook or retweeting on Twitter using their personal social media accounts. However, they should be aware that in doing so they will enable visitors to visit their own accounts and therefore privacy settings should be set to reflect this possibility.
- Staff may not mention the personal social media accounts of pupils or staff via any School social media account, as this exposes the account to the School's followers and may give visitors access to the account mentioned.
- Third party organisations that visit Red House School cannot take photographs of pupils and use them on their social media channels.
- The School may interact via social media with parents, prospective parents and past pupils. Interactions can include photographs; however pupils must not be identifiable by their full name.
- The School can interact via social media with third party organisations, such as clubs which pupils attend outside of School. Interactions can include photographs; however pupils must not be identifiable by their full name.
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.
- The school does not permit staff to accept as friends current pupils on a personal social network site.

TELEPHONE SERVICES

Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles)
- Report the loss or theft of any school mobile phone equipment immediately
- The school remains responsible for all call costs until the phone is reported lost or stolen
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it
- School SIM cards must only be used in school provided mobile phones
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default
- You must not send text messages to premium rate services

- Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so

WRITING AND REVIEWING THIS POLICY

Staff and Pupil Involvement in Policy Creation

Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through a staff working party, consultation through pupil council, draft versions being circulated to all staff and to School Council.

Review Procedure

There will be on-going opportunities for staff to discuss with the e-Safety coordinators any e-Safety issue that concerns them. 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. This policy has been read, amended and approved by the staff, head and governors.

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 person's 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 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 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Reviewed by G Butterfield
Ratified by School Council
November 2020