WOKINGHAM
BOROUGH COUNCIL

Emmbrook Infant School

E-Safety - All in one Model Policy

Responsibility of: Communication, Behaviour and Safeguarding Committee (CBS)

Date of Review: Spring Term 2018

Background

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed we must consider ICT a life-skill.

Most technologies present risks as well as benefits. Internet use for home, social and leisure activities is expanding and being used by all sectors of society. This brings young people into contact with a wide variety of influences, some of which could be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the responsible and safe use of the Internet.

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail and chat all transmit information over the wires and fibers of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Some of the material is published for an adult audience and is unsuitable for pupils. In addition, some use the Web to publish information on weapons, crime and racism that would be more restricted elsewhere. Sadly e-mail and chat communication could also provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Schools need to protect themselves from possible legal challenge. The legal system is still struggling with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers but the possession of other obscene or offensive materials is not clearly covered. The Computer Misuse Act 1990 makes it an offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Schools can help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised".

Risk assessment

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become "E-Safe". Schools need to ensure they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

The school will appoint an e-Safety Coordinator. This role may overlap with the Child Protection Coordinator.

Our Internet Policy has been written by the school, building on the Wokingham Model Policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Why is Internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- *access to world-wide educational resources including museums and art galleries;*
- *inclusion in government nationwide initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);*
- *cultural, vocational, social and leisure use in libraries, clubs and at home;*
- *access to experts in many fields for pupils and staff;*

- *staff professional development through access to national developments, educational materials and good curriculum practice;*
- *communication with support services, professional associations and colleagues;*
- *improved access to technical support including remote management of networks*
- *exchange of curriculum and administration data with the LEA and DfES.*

How will Internet use enhance learning?

Increased computer numbers or improved Internet access may be provided but effective use and quality of learning must also be addressed. Developing good practice in Internet use as a tool for teaching and learning is clearly essential. Teachers need to help pupils learn to extract the meaning from the mass of information provided by the Web. Often the quantity of information needs to be cut down and staff could guide pupils to appropriate websites.

- *The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. (Emmbrook uses the Wokingham Borough filter).*
- *Pupils will be taught what is acceptable and what is not and given clear objectives for Internet use.*
- *Internet access will be planned to enrich and extend learning activities. Access will be reviewed to reflect the curriculum requirements and age of pupils.*
- *Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.*
- *Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.*

How will pupils learn to evaluate Internet content?

Information received via the Web, e-mail or text message also requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read.

Inappropriate material should not be visible to pupils using the Web. This is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may be confronted with inappropriate material, despite all attempts at filtering. Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

More often, pupils will be judging reasonable material but selecting what is relevant to their needs, for instance to answer a homework question. Pupils will be taught research techniques including the use of subject catalogues and search engines. They will be encouraged to question the validity, currency and origins of information – key information handling skills. They will also use alternative sources of information for comparison purposes where available and as appropriate.

1.Roles and Responsibilities

1.1Governors

Governors are responsible for the approval of the e-Safety Policy (including Acceptable Use Agreements), ensuring that it is implemented and reviewing its effectiveness. In fulfilling this responsibility the governing body may choose to appoint an e-safety governor and establish an e-safety committee with appropriate representation. Governors will require/undertake the following regular activities:

- Meetings with the e-Safety Co-ordinator and ICT Strategy team.
- Monitoring of e-safety incident logs.

- Reporting to relevant governor committees.
- Keeping up to date with school e-safety matters.

1.2 Headteacher

The Headteacher is responsible for ensuring the safety, including e-safety, of members of the school community. The day to day responsibility for e-safety may be delegated to the e-Safety Co-ordinator, ICT Subject Leader or another appropriate member of staff. However, the Headteacher will ensure the following:

- Staff with e-safety responsibilities receive suitable and regular training enabling them to carry out their e-safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular monitoring reports.
- There is a clear procedure to be followed in the event of a serious e-safety allegation being made against a member of staff.

1.3 E-Safety Co-ordinator

The e-Safety Co-ordinator has day to day responsibility for e-safety issues and takes a leading role in establishing and reviewing the school e-Safety Policy and associated documents. The e-Safety Co-ordinator will also:

- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide materials and advice for integrating e-safety within schemes of work and check that e-safety is taught on a regular basis.
- Liaise with the local authority.
- Liaise with the school's technical staff.
- Ensure that e-safety incidents are reported and logged and used to inform future e-safety developments.
- Report to the governors and meet with them as required.
- Report regularly to the SLT.

1.4 ICT Technician/Network Manager

The ICT Technician/Network Manager and, where appropriate, the Learning Platform Lead, will, in co-operation with the school's technical support provider, be responsible for ensuring that all reasonable measures have been taken to protect the school's network(s), ensure the appropriate and secure use of school equipment and protect school data and personal information. This will involve ensuring the following:

- The ICT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the e-safety technical requirements outlined in any relevant local authority e-safety policy/guidance.
- Users may only access the school's network(s) through a properly enforced password protection policy, in which passwords are regularly changed.
- The school's filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- E-safety technical information is kept up to date, applied as necessary and passed on to others where relevant.
- Use of the network, learning platform is regularly monitored and any misuse/attempted misuse reported to the e-Safety Co-ordinator or designated person for investigation and action.
- Appropriate steps are taken to protect personal information and secure data on all devices and removable media.
- Provide secure access to the school network from home where necessary using VPN or equivalent technologies.

1.5Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current e-safety matters and the school e-Safety Policy and practices.
- They have read and understood the school's Staff Acceptable Use Policy (AUP) and signed to indicate agreement.
- They report any suspected misuse or problem to the e-Safety Co-ordinator for investigation and action.
- Digital communications with pupils (e-mail/learning platform/voice) should be on a professional level and only carried out using approved school systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's e-Safety and Acceptable Use Policies.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and there is awareness of the procedure for dealing with any unsuitable material that is found in internet searches.

1.6 Child Protection Officer (CPO)

The CPO should be trained in e-safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

1.7 Data Protection Officer (DPO)

The DPO is responsible for maintaining registration with the Information Commissioner's Office, keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.org.uk. SLT should be informed where school policies may require updating.

[See *'Appendix 1 – School and the Data Protection Act'* for further information]

2. Reviewing, Reporting and Sanctions

2.1 Review

- This policy will be reviewed and updated annually, or sooner if necessary.
- The school will audit ICT provision to establish if the e-Safety Policy is adequate and that its implementation is effective.

2.2 Acceptable Use Agreements

- All users of the school computers will sign the appropriate Acceptable Use Agreement. This includes all staff and pupils.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.
- All users will be expected to resign agreements on a regular basis.

2.3 Reporting

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- All pupils and teachers should be aware of these guidelines.
  [See *'Appendix 2 – Course of action if inappropriate content is found'* for further information]

2.4 Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

2.5 Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policies on behaviour, rewards and sanctions.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. This would constitute a disciplinary matter in the case of staff.

3. Communications & Communication Technologies

3.1 Mobile phones and personal handheld devices

- Teacher/parent contact should normally be by the main school telephone and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- All Parent helpers and visitors in school should leave mobile phones with the office staff and collect when they leave.
- Staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises they should arrange temporary cover whilst they make a call.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.2 E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail or messaging accounts will be monitored.
- Staff may access personal web-based e-mail accounts from school but **must not** use these for communications with parents or pupils.
- Under no circumstances should users use e-mail to communicate material (either internally or externally), which is defamatory or obscene.
- Pupils should immediately tell a staff member if they receive an offensive message.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Information of a sensitive nature should not be sent by e-mail.

3.3 Social networking

For the purpose of this policy social networking is considered to be any digital media or medium that facilitates interaction, e.g. Facebook, Twitter, blogs, chat rooms, online gaming, YouTube, Instant Messenger, Second Life, etc.

- Staff have a perfect right to use social networking sites in their private life. In doing so they should ensure that public comments made on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Pupil use of social networking should conform to age restrictions and will not be allowed in school unless this is part of an educational activity and has been authorised by an appropriate member of staff.
- The use of social networking 'tools', e.g. blogs, wikis, messaging, etc., within a school learning platform is both acceptable and to be encouraged.

  [See *'Appendix 3 – Social Networking Guidance'* for further information]

3.4 Internet usage

- Pupils and staff will be informed that internet access will be monitored.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Users must not attempt to disable or reconfigure any filtering, virus protection or similar.
- All pupils using the internet, and associated communication technologies, will be made aware of the school's e-Safety Guidelines. These should be posted near to the computer systems.
- Pupils will receive guidance in responsible and safe use on a regular basis

3.5 Digital and video images

Parents, staff and pupils may record images of pupils at school under the following conditions:

- All staff digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- Images should not be distributed beyond either the school or the immediate family and friends of the pupil's family.
- Images should not be posted on an open internet site, e.g. on a social networking page with the permissions set to public or on the school learning platform and/or website on an open page.
- On the public side of the learning platform and/or website, photographs may only show pictures of children if we have written consent from the parents.
- Pupils' full names may not be used on the learning platform and/or website in conjunction with photographs or video.
- No images of pupils should be recorded
    - in toilets or wash areas
    - whilst pupils are getting changed
    - in the medical room
- The only exceptions to this rule would be if images are recorded to illustrate a particular point for display (e.g. how to wash hands). In this case the line manager must be informed before this activity is undertaken.
- The use of staff devices is not acceptable unless agreed with a member of SLT in advance.
- Images of pupils must be stored securely and deleted when no longer required.

3.6 Learning platform and/or website

- The school learning platform and/or website should include the school address, school e-mail, telephone and fax number including any emergency contact details.
- The school learning platform and/or website should be used to provide information and guidance to parents concerning e-safety policies and practice.
- Staff or pupils' home information should not be published.

- The copyright of all material posted must be held by the school or be clearly attributed to the owner where permission to reproduce has been obtained or given e.g. via Creative Commons licensing.

4. Infrastructure and Security

4.1 Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School ICT technical staff may monitor and record the activity of users on the school ICT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be secured to at least WPA level (Wi-fi protected access).
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician/Network Manager.
- Access to the school ICT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- The 'Administrator' passwords for the school ICT system, used by the ICT Technician/Network Manager are also available to the ICT Subject Leader and must be stored securely in school.

4.2 Passwords

All staff are provided with an individual password. Pupils may have a group password or individual passwords for accessing the network. All users will have an individual log on to the learning platform and/or secure areas of the website.

Clear guidelines will be provided for all users which explain how effective passwords should be chosen. Further expectations of users are detailed below:

- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil.
- Once a computer has been used, users must remember to log off so that others cannot access their information.
- Users leaving a computer temporarily should lock the screen (Windows key + L).
- Passwords should be changed at regular intervals. The school may choose to enforce this requirement through the use of Windows Password Policy where passwords are changed for example every three months.
- In the event that a password becomes insecure then it should be changed immediately.

  [See *'Appendix 4 – Password guidance'* for further information]

4.3 Filtering

The school maintains and supports the managed filtering service provided by RM, the Internet Service Provider (ISP), and the South East Grid for Learning (SEGfL).

- Changes to network filtering should be approved by the ICT Subject Leader and the ICT Technician/Network Manager.
- Any filtering issues should be reported immediately to the ISP and/or SEGfL.

4.4 Virus protection

- All computer systems, including staff laptops/devices, should be protected by an antivirus product which is preferably administered centrally and automatically updated.
- The antivirus product should allow for on-access scanning of files which may be being transferred between computers or downloaded from the internet. In the latter case only dependable sources should be used.
- Staff should have access to and be able to use security software to remove adware and malware.

4.5 Staff laptops/devices

The following security measures should be taken with staff laptop/devices:

- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.
- Laptops/devices should never be left in a parked car, even in the boot.
- Screensavers should be set to lock after a maximum of 15 minutes.
- Laptops/devices should not normally be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

  [See *'Appendix 6 – Exemplar Acceptable Use Agreements and e-Safety Guidelines'* for further information]

4.6 Personal and sensitive data

- All users are responsible for only accessing, altering and deleting their own personal files. They must not access, alter or delete files of another user without permission.
- Sensitive data is any data which links a child's name to a particular item of information and:
  - must be encrypted on laptops/devices, memory sticks, CDs and any other removable media;
  - should not be e-mailed between staff;
  - should be deleted from laptops/devices at the end of an academic year or earlier if no longer required.
- Staff should take care not to leave printed documents with sensitive information open to view, e.g. by not collecting them promptly from printers, or leaving such documents on open desks. Sensitive information should be held in lockable storage when office staff are not present.
- There must be clear procedures for the safe and secure disposal of any device that records data or images, e.g. computers, laptops, memory sticks, cameras, photocopiers, etc.

  [See *'Appendix 5 – Sensitive and Non-Sensitive Data'* for further information]

4.7 Loading/installing software

For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free from viruses.
- Only authorised persons, such as the ICT Technician/Network Manager or ICT Subject Leader, may load software onto the school system or individual computers.

- Where staff are authorised to download software to their own laptops/devices they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

4.8 Backup and disaster recovery

The school will define and implement a backup regime which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur. This regime should include:

- The use of a remote location for backup of key school information, either by daily physical removal in an encrypted format, or via a secure encrypted online backup system.
- No data should be stored on the C drive of any curriculum computer as it is liable to be overwritten without notice during the process of ghosting the computers.
- Staff are responsible for backing up their own data on teacher laptops/devices and should utilise any system that may be enabled such as automated copying of files to the school server.
- Backup methods should be regularly tested by renaming and then retrieving sample files from the backup.

The school should also define a whole school ICT disaster recovery plan which would take effect when severe disturbance to the schools ICT infrastructure takes place, to enable key school systems to be quickly reinstated and prioritised, including who would be involved in this process and how it would be accomplished.

5. E-Safety Education

5.1 Learning and teaching for pupils

- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key e-safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers should be displayed in all rooms and displayed next to fixed site computers.

5.2 Staff training

- Staff will be kept up to date through regular e-safety training.
- Staff should always act as good role models in their use of ICT, the internet and mobile devices.
- Staff will read the 'Keeping Children Safe in Education' document to ensure they are aware of their responsibilities.

5.3 Parental support

The support of, and partnership with, parents should be encouraged. This is likely to include the following:

- Awareness of the school's policies regarding e-safety and internet use; and where appropriate being asked to sign to indicate agreement.

- Practical demonstrations and training
- Advice and guidance on areas such as:
  - filtering systems
  - educational and leisure activities
  - suggestions for safe internet use at home

Appendix 1 – School and the Data Protection Act

The Seventh Principle of the Data Protection Act (1998) states that:

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

This means that schools must have appropriate security to prevent the personal data held (e.g. for staff, pupils and parents) being accidentally or deliberately compromised.

The implications of this for the school will be the need to:

- Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach.
- Be clear about who is responsible for ensuring information security.
- Ensure that the school has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff.
- Respond to any breach of security swiftly and effectively.

Failure to comply with the Act could result in loss of reputation or even legal proceedings.

Further guidance may be found at www.ICO.org.uk

Appendix 2 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
    - Click on Hector the Dolphin to clear the screen
    - Report the incident to the teacher or responsible adult straight away.
- The teacher/responsible adult should:
    - Ensure the well-being of the pupil.
    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the e-Safety Co-ordinator.
- The e-Safety Co-ordinator will then:
    - Log the incident in the E- safety log book and take any appropriate action.
    - Where necessary report the incident to the Internet Service Provider (ISP) so that additional actions can be taken.

Appendix 3 – Social networking guidelines

Staff conduct

- Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.
- Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents even when the postings are within a 'private' online space.

Access to social networking sites

- Social networking sites should not be used or accessed during school working hours.
- Staff may not use school equipment to access social networking sites.
- If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Privacy

- Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.
- Staff should never be 'friends' with children at the school or past pupils up to the age of 18.
- Staff should not create new links with parents simply because they teach their children.
- Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.
- Any changes to social networking sites and privacy settings should be clearly understood.

Additional considerations

Thought should be given to what the implications of this policy will be for the different groupings within the staff employed at the school, e.g.

- Teacher
- Teaching assistant
- Other support staff, e.g. bursar, site manager, lunchtime supervisors, office staff, cleaners
- Outside agency staff, e.g. sports coaches, music tutors, etc.

Appendix 4 – Password guidance

- Passwords must not be easily guessable by anyone and therefore should not include:
    - Names of family, friends, relations, pets etc.
    - Addresses or postcodes of same
    - Telephone numbers
    - Car registration numbers
    - Unadulterated whole words
- Try to use in a password:
    - A mixture of letters and numbers
    - Punctuation marks
    - At least 8 digits
- Possible ideas are
    - Choose a word which has o and i in and substitute 0 (zero) and 1, e.g. sn0wt1me.
    - Use the initial letters of a familiar phrase, song title etc. and substitute as above.
    - Use a text message abbreviation, e.g. CUL8R

Appendix 5 – Sensitive & Non-sensitive data

Sensitive data will include:

- SEN records such as IEPs and Annual Review records
- Mark sheets and assessments
- Reports and Open Evening comments
- Personal data stored on the school's Management Information System, e.g. SIMS
- Photographic or video material
- Name, address and contact information

Non-sensitive data thus includes:

- General teaching plans
- Curriculum materials
- General correspondence of a non-personal nature

Appendix 6 – Exemplar Acceptable Use Agreements

The following are included as possible starting points in developing appropriate agreements and guidelines for individual schools. It is highly unlikely that they will be suitable without amendment and are also likely to require consultation with the respective stakeholders.

The exemplars included are:

- Student/Pupil Acceptable Use Agreement
- Parent/Carer Acceptable Use Agreement
- Exemplar Laptop Acceptable Use Agreement
- Staff Code of Conduct

Student/Pupil Acceptable Use Agreement

For my own personal safety:

- I understand that my teachers will tell me what equipment and software I can use in school.
- I will not tell anyone my username or password except my teachers and family, and will not use any body else' username and password.
- I will immediately click on Hector and tell an adult if I see anything that I don't like or that makes me feel uncomfortable.
- I will only click on apps and games that I have been given permission to by my teachers.

Respecting everyone's rights to use technology as a resource:

- I understand that the school ICT systems are for my learning and that I will not use them for anything else.

Acting as I expect others to act toward me:

- I will respect others people's work and property and will not touch anybody else' work of folders.
- I will be polite and responsible when I communicate with others.
- I will not take or use photographs of anyone without permission.

Keeping secure and safe when using technology in school:

- I will not try to upload, download or access any materials that I haven't been told to.
- I will immediately report any damage or faults involving equipment or software.
- I will not install or attempt to install any new programmes of any type on a machine.
- I will immediately tell a staff member if I receive a message I do not like.
- I will only use the computers for my learning.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- Where work is protected by copyright, I will not try to download copies (including music and videos).

Taking responsibility for my actions, both in and out of school:

- I will treat the computers and i=pads with respect at all times.
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also mean that I cannot use the school network/internet.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

Parent/Carer Acceptable Use Agreement

The school seeks to ensure that *students/pupils* have good access to ICT to enhance their learning and, in return, expects *students/pupils* to agree to be responsible users. A copy of the *Student/Pupil* Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

==========

Acceptance of Use Form

Parent/Carer's Name:	
Student/Pupil's Name:	

As the parent/carer of the above *student/pupil*, I understand that my son/daughter will have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signature:	
Date:	

Exemplar Laptop/Devices Acceptable Use Agreement

1. Introduction

- This agreement applies to all laptops and other associated devices which are loaned to staff and therefore remain the property of the school.
- It should be read in conjunction with the school's e-Safety Policy
- All recipients and users of these devices should read and sign the agreement.

2. Security of equipment and data

- The laptop and any other equipment provided should be stored and transported securely. Special care must be taken to protect the laptop and any removable media devices from loss, theft or damage. Users must be able to demonstrate that they took reasonable care to avoid damage or loss.
- Staff should understand the limitations of the school's insurance cover.
- Government and school policies regarding appropriate use, data protection, information security, computer misuse and health and safety must be adhered to. It is the user's responsibility to ensure that access to all sensitive information is controlled.

3. Software

- Any additional software loaded onto the laptop should be in connection with the work of the school. No personal software should be loaded.
- Only software for which the school has an appropriate licence may be loaded onto the laptop. Illegal reproduction of software is subject to civil damages and criminal penalties.
- Users should not attempt to make changes to the software and settings that might adversely affect its use.

4. Faults

- In the event of a problem with the computer, the school's ICT Technician/Network Manager should be contacted.

Declaration:

I have read and understood the above and also the school's e-Safety Policy and agree to abide by the rules and requirements outlined.

Name:	
Signature:	
Date:	

Staff Code of Conduct

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of pupils, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the school e-Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with pupils (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that pupil use of the internet is consistent with the school's e-Safety Policy.
- When working with pupils, I will closely monitor and scrutinise what pupils are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding pupils' safety to the appropriate person, e.g. e-Safety Co-ordinator and/or SLT member.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:	
Signature:	
Date:	

Acknowledgements:

- Radstock Primary School
- Kent County Council
- 360° Safe – School e-Safety Self- Review Toolkit

Additional information:

This policy should be read in conjunction with national standards and other relevant school policies, procedures and guidelines;

- Safeguarding/Child Protection
- Behaviour Policy
- Teaching & Learning
- Complaints Procedure
- Staff Handbook
- Teachers' Standards (DfE, 2012)