The Keys Academy Trust

Data and e-safety policy

Date: November 2016

Review: Autumn 2018

Earley St Peters C of E Primary School

Data and e-safety Policy

Aim

The aim of this policy is to describe how the school will ensure the safety of pupils whilst using the internet and associated technologies.

Introduction

E-Safety encompasses all technologies including the Internet, mobile phones, digital cameras as well as collaboration tools and personal publishing. It highlights the need to educate staff and pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their technology experiences.

This Data & e-Safety Policy is written to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's Data & e-Safety policy will operate in conjunction with other policies including those for Behaviour, Disciplinary, Anti- Bullying, Curriculum and Data Protection.

Our Data & e-Safety Policy has been written by the school, following guidance from Wokingham Borough Council, Kent County Council and government guidance. It has been agreed by the senior leadership team and approved by the governors.

1. Roles and Responsibilities

Governors

Governors are responsible for the approval of the Data & e-Safety Policy and for reviewing the effectiveness of the policy. There should be a member of the governing body whose responsibility includes:

- Regular meetings with the e-Safety Co-ordinator
- Regular monitoring of e-safety incident logs
- Reporting to relevant Governors committees
- Keeping up to date with school e-Safety matters

This is reported through the Governor Representative on the ICT strategy group.

Headteacher and LMT

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety may be delegated to the Computing Leader or ICT Strategy Group, if necessary.
- The Headteacher /LMT are responsible for ensuring that such staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues when necessary.

- The Leadership Management Team receive and monitor regular reports regarding e-safety.
- The Headteacher and another member of LMT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The School Business Manager, under the direction of the Headteacher, ensures that the Information Commissioner's Office, ICO, registration is kept up to date on an annual basis.

E safety co-ordinator

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents in conjunction with the ICT Strategy Group
- Ensures that all staff, including parent helpers, are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-Safety developments (kept in the safeguarding file)
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant committee meetings of Governors
- Reports regularly to LMT
- Reminds class teachers to display e-Safety rules in the classroom at all times and discuss with pupils at the start of each school year
- Ensures all staff, pupils and parents sign AUP annually

ICT Technician and ICT Subject Leader

In co-operation with the school's technical support provider they are responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the e-Safety technical requirements outlined in any relevant Local Authority
- Safety Policy and guidance
- Users may only access the school's networks 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 that its implementation is not the sole responsibility of any single person
- They keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant

- The use of the network, learning platform and pupil email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety co-ordinator for investigation and action
- Appropriate steps are taken to protect personal information , including the encryption of removable devices including laptops and external storage devices, and the provision of secure access to the school network from home using VPN technologies
- E-safety reminder cards are displayed on all computers
- E-Safety rules are displayed at all ICT access points

Staff

All staff are responsible for ensuring that:

- They are familiar with current e-safety matters and of the school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP) annually
- They report any suspected misuse or problem to the ICT Subject Leader for investigation and action. The ICT Subject Leader will inform the e-safety co-ordinator if necessary.
- Digital communications with pupils (email/Virtual Learning Environment (VLE)/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 e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age
- 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 hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that they are aware of the procedure for dealing with any unsuitable material that is found in internet searches

Child Protection Officer (CPO)

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

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Data Protection Officer

Responsibilities include:

- Maintaining registration with the Information Commissioner's Office
- Keeping abreast of regulatory requirements and recommendations as outlined on their website at www.ico.gov.uk
- Informing staff and LMT of these recommendations so that school policies may be updated. See Appendix 1 – School and the Data Protection Act for further information and the School Data Protection policy

2. e-Safety within learning and teaching

Why new technology use is important

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

Internet use to enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will work with Wokingham Borough Council, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law

Addressing E-safety

- Key e-safety messages are reinforced as part of a planned programme of assemblies, PSHE activities or other curriculum opportunities where appropriate
- Pupils are taught in all appropriate lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the AUP (Acceptable Use Policy) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of computers are displayed in all rooms and displayed next to fixed site computers and attached to mobile devices such as tablets and laptops
- Staff should act as good role models in their use of ICT, the internet and mobile devices as highlighted
- Staff will be kept up to date through regular training in e-Safety

3. Network Security

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented by those responsible.
The Computing subject leader and ICT technician review Earley St Peter's Primary School's ICT systems capacity and security regularly. Virus protection through Sophus is updated daily and additional technical support is provided by independent ICT companies (currently Exceedia, Capita and Waterman Solutions). Security strategies are reviewed, discussed and updated on the advice of Wokingham Borough Council ICT advisors.

- All staff have an individual password. Pupils may have a group password or older pupils may be given individual passwords for accessing the network.
- It may be necessary to have a username with limited access whose password is known to more than one member of staff.
- All users have an individual log on to the Learning Platform.
- 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.
- The "administrator" passwords for the school ICT system, used by the ICT Technician are also available to the ICT Subject Leader and School Business Manager and stored securely in school.
- The school maintains and supports the managed filtering service provided by SEGfL.
- Changes to network filtering should be approved by the ICT Subject Leader and ICT technician.
- Any filtering issues are to be reported immediately to SEGfL.
- School ICT staff may monitor and record the activity of users on the school ICT systems and users are made aware of this through the Acceptable Use Policy.
- The school keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Pupil access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Pupils will not access the Internet without an adult present.
- Parents are asked to sign and return a consent form, (Pupil AUP).

4. School password protocol

- All passwords used by adults should follow the guidelines in this policy.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a child.
- No individual should tell another individual their password.
- 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.
- Passwords must be changed every term and must meet complexity requirements. A security setting determines whether passwords meet these requirements. These requirements are enforced when passwords are changed or created. The minimum requirements are that a password must:
    - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - Be at least six characters in length
    - Contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphabetic characters (for example, !, $, #, %)
- Passwords must not be easily guessable by anyone.
- If a password is identified as insecure then it is essential that the password is changed immediately.

5. Loading software

- Only the ICT Subject Leader or those acting specifically on their behalf such as the ICT Technician are allowed to give consent to staff to install software on school devices. The School Business Manager may load administration Software.
- For the purpose of this policy, software relates to all programs, images or screensavers, which can be downloaded or installed from other media.
- Images and video clips may be downloaded as long as the teacher in charge is satisfied that they are not breaching copyright and data protection laws
- Software loaded on to any school system must be
    - Properly licensed.
    - Free from viruses.
    - Authorised by the ICT Subject Leader

6. Virus Protection and Transferring and downloading files

All computer systems, including staff laptops, are protected by the Sophus antivirus product which is administered centrally and automatically updated.
Great care, by all staff and pupils, should be taken when copying files from one computer to another as there is considerable risk of viruses infecting the school computers. This includes downloading files from the internet where only dependable sources should be used.

7. Security of Sensitive Data

Sensitive data is any data which links a child's name to a particular item of information. Examples include:

- SEN records such as IPPs and Annual Review records.
- Marksheets and assessments.
- Reports and Open Evening comments.
- Personal data stored on the School Information Management System, 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.
- 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.
- Data may be encrypted through full hard-drive encryption using Bitlocker.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Sensitive data
    - Must be encrypted on laptops or memory sticks. All teachers have access to these.
    - Should only be emailed using encryption protocols.
    - Should not be put on a USB stick, CD or any other removable media unless it is encrypted.
    - Should be deleted from laptops at the end of an academic year and archived on the school server

8. Email and messaging guidance

- Staff (including supply staff) and pupils may not use personal web based email accounts from school; bearing in mind that web based email cannot be monitored for unsuitable content.
- Pupils should immediately tell a teacher if they receive an offensive e-mail or message or find an inappropriate web page.
- 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.
- Emails sent by pupils to an external organisation should be authorised by a member of staff before sending.
- The forwarding of chain letters, jokes etc is not allowed.
- Pupils may only use approved e-mail or message accounts on the school system.
- Information of a sensitive nature should not be sent by email.

9. Confidential Information on Laptops

In addition to the information above the following security measures should be taken with staff
laptops:

- Laptops must be out of view and preferably locked away overnight particularly when left at school
- Windows should be locked when a teacher user leaves their computer (Windows key + L)
- Staff and school laptops should never be left in a parked car, even in the boot.
- At home, the families of members of staff should not use a school laptop perhaps allowing access to confidential information. If others are to use the laptop, they should logon as a separate user without staff privileged access.

10. Confidential Information on Paper

Staff should take care not to leave printed documents with sensitive information open to view eg 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.

11. Backing up of data

- The school has a secure on-site and remote backup regimes which will enable recovery of key systems and data within a reasonable timeframe should a data loss occur.
- Data held on individual curriculum systems is liable to be overwritten without notice during the process of ghosting the computers. It is essential that no data is stored on the C drive of any curriculum computer.
- Staff are responsible for backing up their own data on staff laptops if they decide not to use automatic synchronise option. They may copy files to the server for automatic backing up.
- Backup methods are regularly tested by renaming and then retrieving sample files from the backup.
- Earley St Peter's Primary School has 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.

12. The School Learning Platform

- The school Learning Platform includes the school address, school email, telephone and fax number.
- Staff or pupils' home information should not be published.
- Photographs of children are only shown with parental approval (see appendix 3).
- Pupils' full names are not used on the learning platform in conjunction with photographs.

- 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 eg danosongs.com.
- The headteacher takes overall editorial responsibility and ensure that content is accurate and appropriate.

13. World Wide Web

- 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.
- All pupils using the World Wide Web must be made aware of the school's e-Safety Guidelines. These are posted next to all computer access points and frequent reminders are given through lessons and assemblies.
- Instruction in responsible and safe use will precede Internet access on a regular basis (at least once each term).
- Pupils and staff will be informed that Internet access will be monitored.
- Filtering will be carried out by RM (Research Machines) as part of the managed service.
- The school audits ICT provision to establish if the Data & e-Safety policy is adequate and that its implementation is effective through 'stop-check' questioning around the school.

14. Course of action if inappropriate content is found

- If inappropriate web content is found (ie that is pornographic, violent, sexist, racist or horrific) the user should
    - Turn off the monitor or minimise the window immediately
    - Report the incident to the teacher or responsible adult.
- The teacher 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 and take any appropriate action.
    - Where necessary report the incident to our Internet Service Provider (RM) so that action can be taken.

15. The use of new technologies

- Pupils and staff will not be allowed access to public or unregulated chat rooms in school.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Teacher's personal mobile phones may not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

16. Staff use of Social Networking

- Staff have a perfect right to use social networking sites but not during the school day on the school computers.
- Staff should ensure that any public comments they make on social networking sites are compatible with their role as a member of staff and that they show the highest standards of professional integrity.
- Staff should not post photographs of children from the school on their social networking site.
- Staff should regularly check their profile settings on social networking sites to ensure that
    - No pupil (or recent past pupil (under 16)) is able to see extra material that is not public (eg not be a friend or a contact).
    - No parent of a child at school should be able to see extra material that is not public.
    - Any changes to social networking sites and privacy settings are clearly understood.

17. Child use of Social Networking sites

- Pupils at school are regularly educated in e-Safety which includes the safe use of social networking sites.
- Pupils are able to use the learning platform at school and at home, which has some aspects of social networking. One key feature of the learning platform is the ability to control, filter and check the flow of information through the system.
- Most social networking sites are blocked at school. However, to further the pupils' education in the use of such sites they may be unblocked for specific activities on specific occasions. This is undertaken with the knowledge of the ICT subject leader and ICT Technician (who unblocks and re-blocks the sites).

18. Use of mobile device

- Pupils are not allowed to bring mobile phones to school unless parents make prior arrangements with the school. Pupils' personal mobile phones must be stored in the school office throughout the school day.
- Pupils are not allowed to bring in games devices which allow ad hoc networks to be established.
- 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.
- Staff, helper and visitor mobile devices should normally be switched off or on silent during the times that children are present.
- Staff and Parent helpers in school 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.
- The sending of abusive or inappropriate text messages is forbidden.
- Schools should be vigilant where mobile phones are used with children in the Foundation Stage.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.

19. Photography of pupils

- Parental permission
    - The school will ensure that appropriate written permissions are obtained for the taking and use of digital and video images of pupils. Such use could include the school website, learning platform, display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press
    - If specific individual pupil photographs are to be used publically, such as on the school website, in the prospectus or any other high profile publication, then a check should be made with individual parents for this additional use
    - Unless specific parental permission has been obtained, pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain. The school will also ensure that pupil names are not used in any file names used to save images; or in tags when publishing online
    - Where parental permission has not been obtained, or is it known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded
- All images of pupils will be securely stored on the curriculum server under the photograph folder in the staff area
    - Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, this must only be for temporary storage until images can be uploaded to the secure central location. The images should then be deleted from the temporary storage location and care taken to ensure they are not still available, e.g. in a recycle bin
    - Images may be retained for up to 6 years after a pupil has left the school and are then deleted in line with the data retention policy
- School digital devices should always be used to record images of pupils
    - All pupils appearing in images should be appropriately dressed.
    - Pupils must not take, use, share, publish or distribute images of others without their permission.
    - Where images are taken using devices with a facility to store or transfer data to other locations (e.g. automatic copying to online cloud storage) care must be taken to ensure such features are disabled.
    - All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.

    - Where volunteers are supporting school staff, they should abide by the same rules as school staff as far as is reasonable.
    - The use of staff's personally owned devices (e.g. staff smart phones, personally owned cameras) to record images is strictly forbidden.
- Where the school chooses to allow the recording of images at public events, the following should apply:

    - Images may only be recorded for personal use and can only be shared with immediate family and friends. They must not be shared on social networking sites or other websites that are accessible to the general public.

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.

    - For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
    - Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
    - Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

20. Acceptable Use Policy and Agreement

- All users of the school computers (ie staff and pupils) should sign the appropriate acceptable use policy or agreement on an annual basis.
- Parents will also be asked to sign the parent / carer acceptable use agreement on an annual basis.

21. Complaints Regarding Internet Use

- The school have procedures in place for dealing with any complaint of Internet misuse.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Complaints of Internet misuse will be dealt with by the headteacher.
- Any complaint about staff misuse will be referred to the headteacher.

22. Sanctions

- The school has a system of sanctions to promote the appropriate use of technology.

- 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 as far as staff are concerned.

23. Parental Support

- Parents are made aware of the school's policies regarding Data & e-Safety and Internet use via newsletters and information evenings.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents is encouraged.
- Parents' attention are informed of the school Data & e-Safety Policy in newsletters, the school prospectus and on the school learning platform.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet is available to parents via the e-safety link on our learning platform.

Date of this policy	November 2016
Date for review	Summer 2018

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.gov.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:
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- 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 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

Specific guidelines relating to staff use of social networking are best arrived at through discussion to both clarify and agree exactly what should be applicable. Aspects will also be applicable to those associated with the school, e.g. governors and parent helpers.

The following areas should be included in any policy:

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 never be accessed during timetabled lessons and other contact with pupils and not normally 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 to personal social networking pages (including blogs and community based forums).
- 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

This guidance is intended for those adults using school systems but is based on good practice and should also feature in the teaching of, and advice to, pupils.

- Passwords should have a 'strength' of at least 12 where a letter is 1 and a number or punctuation mark is 2. The choice of password 'strength' should be appropriate to the data being protected and the potential risks associated with that data being compromised.
- Passwords should avoid following a pattern or being predictable.
- 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
    - Birthdays
    - 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

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 Acceptable Use Agreement

Student/Pupil Acceptable Use Agreement

This agreement will need amending to suit the age of the students/pupils concerned.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, e-mail and other digital communications.
- I will not tell anyone my username or password nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger', when I am communicating online.
- I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online.
- I will not arrange to meet people offline that I have communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

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

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

Acting as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- I will only use my personal handheld/external devices (e.g. mobile phones, USB devices, etc.) in school if I have permission and I understand that if I do use my own devices in school I must follow the rules as if I was using school equipment.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails, unless given permission to do so and I know and trust the person/organisation that sent the e-mail.
- I will ask for permission before sending an e-mail to an external person/organisation
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I receive an offensive e-mail or message.

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.
- I should ensure that I have permission to use the original work of others in my own work.
- 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 understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, 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 include loss of access to 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 Acceptable Use Agreement

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:	