The Colleton Primary School
Colleton Drive
Twyford
Berkshire
RG10 0AX

T (0118) 934 0530
F (0118) 934 4641
E admin@colleton.wokingham.sch.uk
www.colleton.wokingham.sch.uk

e-Safety Policy

1. Roles and Responsibilities

a) Governors

Governors are responsible for the approval of the 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-ordinators (HT & Computing team).
- Regular monitoring of e-Safety incident logs with ML.
- Reporting to relevant Governors committees.
- Keeping up to date with school e-Safety matters, including any e-Safety allegations

b) Headteacher and SLT

- 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 and ICT team or another appropriate member of staff.
- The Headteacher is 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 Headteacher, another member of the Senior Leadership Team and the e-Safety governor 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 Headteacher ensures that the Information Commissioner's Office, ICO, registration is kept up to date on an annual basis.

c) E-Safety co-ordinators (HT & Computing Team)

- Takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents.

- Ensures that all staff 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 through staff meetings and briefings, briefings for parent volunteers, TA meetings.
- Liaises with the Local Authority.
- iLiaises with ICT support provider Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments which is displayed in the staffroom.
- Meets at least annually with e-Safety Governor to discuss and review significant changes, current issues, review incident logs and filtering/change control logs.
- Attends relevant committee meetings of Governors.
- Reports regularly to the Senior Leadership Team.

d) PSHE co-ordinator/curriculum co-ordinator (BR)

- Provides materials and advice for integrating e-Safety within PSHE schemes of work.
- Checks that e-Safety is taught on a regular basis.

e) The school's ICT support provider is 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 e-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 keep 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, Microsoft Teams and pupil email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety co-ordinator(s) for investigation and action
- Appropriate steps are taken to protect personal information, which may include the encryption of removable devices including laptops and external storage devices, and the provision of secure access to the school network from home

where necessary using VPN or equivalent technologies (installed on school equipment only).

f) Teaching and Support Staff

Teaching and support 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. Master AUP can be found in the appendices of this document.
- They report any suspected misuse or problem to the Computing and ICT Subject Leader for investigation and action.
- Digital communications with learners (messaging through the Teams/Purple Mash/phone call) should be on a professional level *and only carried out using approved school channels.*
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Learners understand and follow the school e-Safety and acceptable use policy, known as the NetSmart Code.
- Learners 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.

Learners understand how to safely use a search engine and why it is important to do so safely.

g) Child Protection Officer (CPO) – (ML + Gov BD)

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.

h) Data Protection Officer – LC & CS

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.gov.uk and informing staff and leadership so that school policies may be updated. Refer to the school's data protection policy on our website.

2. E-Safety within learning and teaching

- Key e-Safety messages are reinforced as part of a planned programme of assemblies, PSHE activities or other curriculum opportunities where appropriate.
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information and be able to consider whether reported information could be fake news.
- Learners should be helped to understand the need for the NetSmart Code (children's AUP) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Learners should be taught to use search engines that they will encounter in the wider world in a safe manner and to understand why this is an important skill.
- All internet browsers accessed by pupils should have the school website as the home page, and Google and Wonde as tabs.
- The NetSmart Code for use of computers is displayed in all rooms and displayed next to fixed site computers.
- Staff should act as good role models in their use of ICT, the internet and mobile devices including smart watches.
- Staff will be kept up to date through regular training in e-Safety.

3. Network and Microsoft Teams Security

The school will be 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.

- All staff & governors have an individual password. Pupils have a group password or older pupils may be given individual passwords for accessing the network.
- All users have an individual log on to Teams that is age appropriate.

- Reg Group Teachers will keep password lists for children in their team secure.
- If a child thinks someone may know their password, they should inform their teacher who will arrange for a new one to be created as soon as possible.
- Access to servers, and communications cabinets is 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 school ICT support contractor.
- The "administrator" passwords for the school ICT systemare stored securely by our ICT support contractor.
- The school maintains and supports the managed filtering service provided by SEGfL.
- Changes to network filtering should be approved by the Computing Team.
- Any filtering issues are to be reported immediately to SEGfL.
- School 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.

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 (ctrl/alt/del then press K on Windows XP; for Windows 7 and Netbooks, select 'lock' from the Start menu or press ctrl/alt/del and select 'lock'.)
- Passwords must not be easily guessable by anyone and should ideally be a combination of letters and numbers.
- They 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 I and O in and substitute 1 and 0 (zero) eg sn0wt1me.
    - Use the initial letters of a familiar phrase, song title etc. and substitute as above.
    - Use a text message abbreviation CUL8R for instance- but nothing obvious like this example.
- If you know your password is insecure then it is essential that the password is changed immediately.

5. Loading software

- Only the Computing Team, or those acting specifically on their behalf are allowed to load software on to any school computer or device.
- 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.
- Software loaded on to any school system must be
    - Properly licensed.
    - Free from viruses.
    - Authorised by the Computing Team and ICT Subject Leaders, ICT TSupport contractor or Network Manager

6. Virus Protection

- All computer systems, including teacher laptops, are protected by an Antivirus product which is preferably administered centrally and automatically updated. This is managed by ICT support contractor.
- Any virus, adware or malware incidents should be reported immediately to the ICT support contractor.

7. Transferring and downloading files

Great care 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. Use of a site-wide virus protection program with on-access scanning is enabled.

8. School handling and security of Sensitive Data – See Data Protection Policy

9. Email and messaging guidance

- Staff but not pupils may use web-based email accounts from school; bearing in mind that web-based email cannot be monitored for unsuitable content.
- Teachers' and governors school email addresses should not be included in emails to parents unless they are under BCC unless prior agreement has been given by the staff member (this can permission be retracted if it is not be using appropriately).
- 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 and jokes are prohibited in school.
- pupils may only use approved email or message accounts on the school system.

10. Confidential Information on Laptops

In addition to the information above the following security measures should be taken with teacher laptops or Chromebooks.

- they must be out of view and preferably locked away overnight particularly when left at school.
- Windows desktops should be locked when a teacher user leaves their computer (Windows key + L)
- they should never be left in a parked car, even in the boot.
- At home, other members of teachers' families should not use a teacher's device perhaps allowing access to confidential information.

11. Confidential Information on Paper

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.

12. Backing up of data

- Data held on individual curriculum systems is liable to be overwritten without notice during the process of ghosting the computers. Staff should note no data is stored on the C drive of any curriculum computer.
- Data held on individual iPads is liable to be overwritten without notice during the process of re-imaging the iPads. Any data which needs to be kept (especially photos, videos etc.) should be uploaded to the appropriate shared drive/Teams as soon as possible.
- Staff are responsible for backing up their own data on teacher laptops. They may copy files to the server for automatic backing up.
- Regular / Daily backups of our servers (physical and virtual) are taken using a secure off-site backup system. There is no need for any action to be taken by the school once the schedule is set up. In addition to data held on our shared drives, the following systems backed up are also backed up: SIMS, SCO (Tucasi), Microsoft Exchange (Email).
  (See attached Computer Issues for details)
- Emails are sent to the School Business Manager informing of the success or otherwise of the backups. Our Support Contractor also gets a copy of the email.

A whole school ICT disaster recovery plan is part of the Business Continuity Plan found in the Rainbow Plan folder.

13. The School Website

- The school website should include the school address, school email and telephone including the school's emergency email address.
- Staff or pupil's 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 eg via Creative Commons licensing where appropriate.
- See **Photography of Pupils** for detail concerning the use of photographs.

14. Use of the Internet

- 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 learners using the World Wide Web must be made aware of the school's NetSmart Code. These should be posted near to the computer systems.
- Instruction in responsible and safe use will precede Internet access on a regular basis (at least once each term).
- Learners 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, aided by the computing and PSHE subject leaders, will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

15. 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 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 officer.
  - The e-Safety officer will then
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to the Internet Service Provider (RM) so that action can be taken.

16. Staff use of Social Networking

- Staff have a perfect right to use social networking sites.

- Staff should ensure that 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 their class on their social networking site.
- Staff should check their profile settings in 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

- Learners will not be allowed to access public or unregulated chat rooms.
- Learners at school are regularly educated in e-Safety which includes the safe use of social networking sites.
- Learners are able to use Teams at home, which may have some chat functions. Where this is available staff members will have access to all messages at all points in time for monitoring purposes.

18. Use of mobile devices

- Learners are not allowed to bring mobile phones or other electronic devices such as Kindles, tablets or iPads to school unless prior arrangements are made with the school and the device must be handed to their registration teacher for safe-keeping each day.
- Pupils are not allowed to bring in games devices including those on watches, such as Vtech or similar.
- Teacher/parent contact should normally be by the main school telephone or office email and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- Parent helpers in school and staff must ensure that they do not send or receive 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, helper and visitor mobile devices should be switched off or on silent during the times that children are present. This includes notifications on smart watches.
- No device in any of the school buildings should contain any content that is inappropriate or illegal.
- Mobile phones and watches enabled with similar functionality should only be used in the office, staff room or PPA room during normal school hours. During pandemic restrictions phones may be carried at all times but only used in emergency situations to contact the school office or a member of SLT for support.

19. Photography of pupils - general

- Learners' full names will not be used in conjunction with photographs on the public part of Microsoft Teams, social mediaor school website.
- Only photographs of learners whose parents have given permission for them to appear on our website or in social media will be used.
- Staff will check the Photograph list to ensure that no photograph of a learner without permission is used.
- Names can be used in conjunction with photos on the password protected parts of Microsoft Teams.
- Where possible school devices should be used for work. Where this is not possible staff personal devices are being used for school purposes, consideration must be given to the security of images/data in case of loss of the device e.g. photos should be downloaded in school and removed from the camera or memory card.
- Photographs are to be kept on Microsoft Teams organised by academic year with subfolders for each team and one for staff. Using this system photographs can and will be easily deleted within a year of the children leaving Older Team.
- Photographs taken by the newspaper have parents' permission to publish names unless included on the Photograph list.

20. Photography of pupils – parents

- Parents may take photographs of their children during sports events and following any performances but they should not be posted on social networking sites with permissions set to public.
- Parents' permission for the use of photographs is requested as part of the school induction pack.

21. Photography of pupils – staff and pupils

- Only school cameras should be used. If own cameras are needed e.g. on trips, photographs must be downloaded in school immediately on return and removed from own camera.
- All devices capable of taking photographs, whether belonging to the school or personal, may be subject to scrutiny by managers if required.
- It is the staff's responsibility to ensure children without permission are not photographed for any newspaper.

22. Acceptable Use Policy and NetSmart Code

- All staff users of the school computers and laptops will sign our Acceptable Use Policy (Refer to Appendix1).
- Learners' NetSmart Code of Practice and SMART code should be discussed termly in teams where the Internet is in use, and displayed clearly in all Teams and the e-classroom. During the course of Computing lessons, all learners will be taught how to use technology safely when using the internet at home and at school, even if they are not required to use the Internet. The NetSmart Code of Practice will be sent out electronically to parents and carers of all KS1 and KS2 children at the beginning of each school year so they can confirm their children will follow the guidelines as set out.

23. Complaints Regarding Internet Use

- Any complaints regarding Internet misuse will be dealt with in accordance with the school Behaviour Policy.
- 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.
- Where appropriate, incidents will be entered in the e-Safety log.

24. Sanctions

- A system of appropriate sanctions will be used to promote the safe use of technology within school. E.g. Suspension of privileges, individual access to Microsoft Teams, school PCs etc.

- 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.

25. Parental Support

- Parents will be made aware of the school's policies regarding e-Safety and Internet use through e-Safety meetings, newsletters and, where appropriate, Microsoft Teams.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet may be made available to parents as appropriate.

Personal Device use for work outside of School

- The preferred method of storage for all work documents is Microsoft Teams however due to the limitations of the system it understood that some documents that contain no sensitive information may need to be stored on Staff Members personal devices for short periods of time before being deleted.
- Whilst using a personal device for work purposes staff members should ensure that they are only carrying out work tasks to reduce the risk of personal and sensitive data leaking onto the school system. All work applications should be closed when work is completed.

To be read in conjunction with the "Bring your own device" policy.

Responsibility: Curriculum Committee
Written by: WBC/Computing Team
Reviewed: Bi-annually
Last Review: May 2021
Next Review: May 2023
Ratified: 26th May 2021

Appendix 1: Code of Conduct – Acceptable Use Policy

Staff Professional Responsibilities in the use of ICT

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.

1. I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
2. I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
3. I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
4. I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
5. I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
6. I will not install any software or hardware without permission.
7. I will ensure that personal data, particularly that of students, 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.
8. I will respect copyright and intellectual property rights.
9. I will ensure that electronic communications with pupils (including email, 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.
10. 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.
11. I will ensure that pupils only use the Internet when given permission by a member of teaching staff. Any use of computers at lunchtime must by supervised by a teacher or teaching assistant who is present in the team areas.
12. I will only use my mobile phone in the office, staffroom or PPA rooms during school hours (areas not accessed by children).
13. 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.

14. I will ensure that computer monitor screens are readily visible, to enable monitoring of what the children are accessing.
15. I know what to do if offensive or inappropriate materials are found on screen or printer.
16. I will familiarise myself with all monitors and devices so that the screens can be blanked should inappropriate material appear.
17. I will report any incidents of concern regarding pupils' safety to the e-Safety Coordinator, the Designated Child Protection Officer or Headteacher.
18. I have read and understood the Colleton Primary School e-Safety Policy

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 (capitals)	Signature	Date
Staff Member			
Headteacher			
Student			
Regular Voluntary Helper			