SINGLEWELL SCHOOL

Curriculum

Internet Acceptable Use

Document Title	Internet Acceptable Use
Policy Status	
Date of Issue	February 2024
Date to be Revised	February 2025

Approved: ___________________

Intent for Computing Curriculum

Computing has become a major aspect of learning and education with the impact and benefits of computing systems permeating many areas of daily life. At Singlewell Primary School, we aim to develop 'thinkers of the future' through a modern, ambitious and relevant education of computing. We aim to provide the children with the skills they need to navigate the wider computing curriculum, as well as the knowledge they need to be resilient and adapt to new technology. Being safe is the primary concern when using computing systems and we will ensure that all children will have the necessary knowledge and experience to navigate through the digital world safely and productively. We aim to instil a sense of curiosity and fun when using computing systems, where problem solving becomes enjoyable and engaging. Our curriculum coverage also instils a sense of responsibility for being equal and productive when acting online and we aim to link the many aspects of computer usage with real day to day life. The computing curriculum at Singlewell Primary School provides a strong, secure platform of learning for the children to advance long into their academic and personal futures, incorporating aspects of computer programming as well as the tools they will need to traverse and utilise the internet for inspiration and wider learning.

This policy forms part of the Computing Policy of Singlewell School.

Our policy has been written by the school, building on the Kent NGFL policy and Government guidance.

1. **<u>The importance of the Internet</u>**

- The purpose of Internet use in school is to raise the education standards, to promote pupil achievement, to support the professional work of the staff and to enhance the school's management information and business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.

2. **<u>Benefits of the Internet</u>**

   Benefits of using the internet in education include:

- Access to worldwide education sources, including museums and art galleries
- Educational and cultural exchanges between pupils worldwide
- 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.
- Mentoring of pupils and provide peer support for them and teachers.
- Opportunity to reduce workload through careful use of AI tools.

3. **Using the internet to enhance learning**

- The school internet access will be designed expressly for pupils use and will include filtering, appropriate to the age of the pupils.
- Pupils will be taught what internet use is acceptable and what is not and will be given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement and age of pupils.
- Staff should guide pupils to 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, retrieval and evaluation.

4. **Evaluating Internet content**

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the I.C.T co-ordinator.
- Schools should ensure that the use of internet derived materials by staff and by pupils complies with copy right law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information.

5. **E-Mail Management**

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive email communication, such as address or telephone number exchange, or arrange to meet anyone.
- Whole class or group e-mail addresses should be used at KS2 and below.

6. **Management of Website**

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not appear anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The website should comply with the school's guidelines for publications.

7. **E-Mail Lists**

- Newsgroups will not be made available to pupils unless an education requirement for their use has been demonstrated.

8. **Using chat Rooms**

- Pupils will not be allowed to access public or any unregulated chat rooms.

9. <u>Managing emerging Internet Applications</u>

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

10. <u>Internet Access</u>

- The school will 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.
- At KS1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form.
- Primary pupils will not be issued individual e-mail accounts, but will be authorised to use a group / class e-mail address under supervision.

11. <u>Risk Assessment</u>

- In common with other media such as magazines, books and videos, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that the users access only appropriate material. However due to the international scale and linked nature of the Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or use for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, access and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the internet policy is implemented and compliance with the policy monitored.

12. <u>Protected Access</u>

- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

13. <u>Policy Access for:</u>

a) **Pupils**

- Rules for the internet access will be posted in all rooms where computers are used.
- Pupils will be informed the internet use will be monitored. Instruction in responsible and safe use should precede Internet access.

b) **Staff**

- All staff must accept the term of the 'Responsible Internet Use' statement before using any internet resource in the school.
- All staff including teachers, supply staff and support staff will be provided with the school Internet policy and its importance explained.

14. <u>System Security</u>

- The school computing systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the LEA, particularly where a wide area network connection is being planned.

15. <u>Complaints</u>

- Responsibility for handling incidents will be delegated to a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher.

16. <u>Parental Information</u>

- Parents' attention will be drawn to the School Internet Policy in Newsletters, the School Brochure and on the School Website.
- Internet issues will be handled sensitively to inform parents without undue alarm.

Using ICT at School and Home Safely

As part of your child's curriculum and development of computing skills, Singlewell School is providing supervised access to the internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. We have forms stating the schools rules for Responsible Internet Use which we ask that parent/carers sign and return to the school office so that your child may use the internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school internet provider operates a filtering system that restricts access to inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the internet. The school will not be liable for any damages arising from your child's use of the internet facilities.

The rules our School follow when using the internet are:

- **Key Stage 1**
  - We only use the internet when an adult is with us
  - We can click on the buttons or links when we know what they do
  - We can search the internet with an adult
  - We always ask if we get lost on the Internet
  - We can send and open e-mails together
- **Key Stage 2**
  - We ask permission before using the internet
  - We only use websites that an adult has chosen
  - We tell an adult if we see anything we are uncomfortable with
  - We never give out personal information or passwords

Further advice for parents/carers

Singlewell School is committed to promoting the safe and responsible use of the internet and as such we feel it is our responsibility to raise this particular issue as a concern. Websites such as Facebook offer amazing communication and social connections, however they are created with their audience in mind and it is not possible to control or verify the content.

Facebook and similar social media sites terms and conditions state that all users must be 13 years or older and as such we strongly recommend that parents do not allow their children to have their own personal profiles online.

Possible risks for children under 13 using Facebook/social media may include:

- Facebook use "age targeted" advertising and your child could be exposed to adverts of a sexual or other inappropriate nature.
- Children may accept friend requests from people they don't know in real life which could increase the risk of inappropriate contact or behaviour.
- Language, games, applications, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal, or unsuitable for children.
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy setting and inappropriate behaviour.
- Facebook cannot and does not verify its members therefore it is important to remember that if your child can lie about who they are online, so can anyone else!

We feel it important to point out to parents the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from school and sometimes by a child, their friend, siblings or even parents. We will take action (such as reporting underage profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children.

We are however aware that many children do use such sites and it is possible that by banning access and removing children's technology may mean that children do not feel able to raise any concerns or problems encountered with parents / carers or in adults in the school. It is also important that parents/carers are aware that whilst filtering tools or parental controls are very useful in keeping children safe online, they are not always effective and children may still access unsuitable content.

However, if you should decide to allow your child to have a profile/account on social media, we strongly advise you to be aware of the potential risks posed to your child. You may want to consider the following points:

- Check their profile is set to <u>private</u> and that only approved friends can see information that is posted
- Closely monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information, clicking on

unknown links, installing applications, and not posting offensive messages or photos.

- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application on www.facebook.com/clickceop on a Facebook profile.
- Set up your own profiles on sites being used by them so you understand how the sites works and ask them to have you as a friend on their profiles so you know what they are posting online. Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents
- Make sure your child understands the following rules:
  - Always keep your profile private and never accept friends you don't know in real life
  - Never post anything online which could reveal your identity or anything you wouldn't want your parents to see
  - Only click on links that you trust and always ask an adult if at first you are not sure
  - Never agree to meet somebody you only know online without telling a trusted adult
  - Always tell an adult you trust if you feel threatened, see something that makes you feel worried or someone upsets you online.

We recommend that all parents visit 'CEOPs Think U Know' website for more information on keeping your child safe online www.thinkuknow.co.uk

Further advice and information can also be found at www.kent.gov.uk/esafety

Approved: ___________________

SINGLEWELL SCHOOL

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before I use the Internet
- I will use only my own Internet login and password, which is secret.
- I will only look at or delete my own files.
- I understand that I must not bring software or disks into school without permission
- I will only e-mail people I know, or my teacher has approved
- The messages I send will be polite and sensible
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know
- I will not use Internet chat
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately
- I understand that the school may check my computer files and the Internet sites I visit
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

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

Approved: ___________________

SINGLEWELL SCHOOL

Acceptable Use Policy 2024

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, *unauthorised* access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and computing include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any GDPR of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

Approved: ___________________

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, flash drives, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead Mrs Michelle Brown and/or the Online Safety Coordinator Mr Michael Evans as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead Mrs Michelle Brown and/or the Online Safety Coordinator Mr Michael Evans for filtering as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Computing Lead Mr Michael Evans as soon as possible.

13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

14. I will ensure that my online reputation and use of technology and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, and gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of technology and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP, prevent strategy and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

Approved: ___________________

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead Mrs Michelle Brown and/or the Online Safety Coordinator Mr Michael Evans or the Head Teacher.

18. I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

19. Through the Prevent Strategy, staff at Singlewell work together to divert vulnerable individuals from being radicalised. All staff need to be aware of the risks posed by online activity of extremist and terrorist groups. Staff have a vital role to play in protecting pupils from risks of extremism and radicalisation. To keep children safe from risks posed by terrorist exploitation of social media I will approach it in the same way as safeguarding children from other online abuse.

20. I will not use my personal camera, mobile phone camera or any other photographic device for taking photographs of school pupils or work. Only school cameras or school iPads should be used.

21. Staff are to report to the Data Leader, Sandra Mason, with any data breaches. The Data Leader will inform DPO. Staff are to report breaches within 24 hours to the Data Leader and then the Data Leader will report to the DPO within 72 hours.

22. I understand that if I use an app or any program that uses staff or pupil data I will inform the Data Lead immediately of the name of the program or app.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: .... Print Name: .... Date: ....

Accepted by: .... Print Name: .... Date...........

Letter for Staff

Dear Staff Member

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as "friends" on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this, then please speak to the Online safety (e-Safety) Coordination Leader Mr Michael Evans or Designated Safeguarding Lead Mrs M Brown.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer practise with Technology" are available in the staffroom) to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from www.childnet.com, www.kelsi.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to your line manager, The Computing Leader, Mr Michael Evans or the Designated Safeguarding Lead if you have any queries or concerns regarding this.

Yours sincerely

Mrs M Brown
Headteacher

Approved: ________________

Additional content regarding online participation on behalf the School

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the school then we request that you:

- Be professional and remember that you are an ambassador for the school. Disclose your position but always make it clear that you do not necessarily speak on behalf of the school.
- Be responsible and honest at all times and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Be accountable and do not disclose information, make commitments or engage in activities on behalf of the school unless you are authorised to do so.
- Always inform your line manager, the designated safeguarding lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

Approved: ___________________