Curriculum

ICT and Internet Acceptable Use Policy

Document Title	ICT and Internet Acceptable Use
Policy Status	
Date of Issue	February 2026
Date to be Revised	February 2027

Approved: _____

Contents

1. Introduction, intent and aims..... Error! Bookmark not defined.
2. Relevant legislation and guidance..... Error! Bookmark not defined.
3. Definitions..... Error! Bookmark not defined.
4. Unacceptable use.....4
5. Staff (including governors, volunteers, and contractors).....Error! Bookmark not defined.
6. Pupils..... 7
7. Parents/carers..... Error! Bookmark not defined.
8. Data security..... Error! Bookmark not defined.
9. Internet access..... Error! Bookmark not defined.
10. Social Media..... Error! Bookmark not defined.
11. Monitoring and review..... 10
12. Related policies.....12
Appendix 1: Rule for responsible use of ICT and the internet for EYFS/KS1.....Error! Bookmark not defined.
Appendix 2: Rules for responsible use of ICT and the internet for KS2 ..... Error! Bookmark not defined.
Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors..... Error! Bookmark not defined.
Apppemdix 4: Letters to staff concerning Social Media 19

Approved: _____

Intent for Computing Curriculum

At Singlewell Primary School, we recognise that computing is an essential part of everyday life and a vital skill for the future. Our computing curriculum aims to develop **confident, capable and responsible digital learners**, supporting children to become *thinkers of the future* through a modern, **ambitious** and relevant computing education.

Our curriculum is designed to reflect our **CARES school values**, promoting **curiosity** and enjoyment when using computing systems, where problem solving is engaging and meaningful. Pupils are encouraged to explore new technologies, think creatively and develop **resilience** by learning from mistakes, persevering with challenges and adapting their thinking when things do not work first time.

Being safe online is a core priority. We aim to ensure that all pupils develop a strong understanding of how to stay **safe** online and behave with respect towards others when communicating digitally. Children are taught to recognise potential risks, protect personal information, and understand the importance of digital citizenship.

Using Purple Mash as a core platform, pupils develop essential skills in computer science, information technology and digital literacy. Learning is carefully sequenced to ensure clear progression, enabling pupils to apply their skills across the wider curriculum with increasing independence.

Our curriculum promotes an equal approach to learning, ensuring all pupils have opportunities to succeed, collaborate and express themselves through technology. By linking computing to real-life contexts and cross-curricular learning, we aim to equip pupils with the knowledge, skills and understanding they need to thrive in an increasingly digital society.

1. Introduction and aims

Information and Communications Technology (ICT) is an essential part of how Singlewell Primary School operates. It supports teaching and learning, administration, and pastoral care, and is used by pupils, staff, governors, volunteers, contractors, and visitors.

ICT can also pose risks to data protection, online safety, and safeguarding. This policy aims to:

- Set clear guidelines and rules for using the school's ICT resources for staff, pupils, parents/carers, and governors
- Establish expectations for safe, respectful, and responsible online behaviour for all members of the school community
- Support the school's policies on data protection, online safety, and safeguarding
- Prevent misuse of ICT that could disrupt school operations
- Promote safe and effective use of ICT and the internet as part of teaching and learning

This policy applies to all users of the school's ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors. Misuse may be addressed under the school's behaviour or disciplinary policies.

Approved: _____

2.Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, the following legislation and guidance:

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Human Rights Act 1998
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, Screening and Confiscation: Advice for Schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting Digital and Technology Standards in Schools and Colleges

3. Definitions

ICT: all digital devices, systems, software, applications, websites, web services, and future ICT resources.
Users: anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
Personal use: any activity not directly related to work, study, or school-approved purposes.
Authorised personnel: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
Materials: Files or data created using school ICT, including documents, photos, audio, video, printed output, web pages, blogs, and social media.

4. Unacceptable use

The school's ICT facilities must be used safely, responsibly, and legally. Unacceptable use includes:

A. Respect, Safety, and Behaviour

- Bullying, harassing, or discriminating against others.
- Using offensive, obscene, pornographic, or otherwise harmful material.
- Consensual or non-consensual sharing of nude or semi-nude images, videos, or livestreams.

Approved: _____

- Using inappropriate or offensive language.
- Making statements or posts that defame or bring the school into disrepute.
- Promoting extremist, radicalised, racist, anti-Semitic, or otherwise discriminatory content.

B. Legal and Policy Compliance

- Breaching copyright or intellectual property rights.
- Engaging in illegal activity, or promoting illegal behaviour.
- Participating in online gambling, scams, phishing, or inappropriate advertising.
- Breaching school policies or procedures.
- Promoting a private business unless it is directly related to the school.

C. Network and System Security

- Connecting devices to the school's network without approval.
- Accessing restricted areas, password-protected information, or blocked websites without permission.
- Using software, applications, or tools on the network without authorisation, including anything designed to interfere with systems, accounts, or data.
- Allowing or helping others to gain unauthorised access.
- Removing, deleting, or disposing of school ICT equipment, systems, programs, or information without permission.
- Causing intentional damage to school ICT facilities or equipment.
- Attempting to bypass the school's filtering or monitoring systems.
- Causing a data breach by accessing, modifying, or sharing data without authorisation.

D. Approved Use Only

- Using chat rooms, message boards, blogs, or other online services only without approval from authorised staff.

E. Other Considerations

- This list is not exhaustive. The head teacher (or other authorised staff) may decide that any act or behaviour not listed is considered unacceptable use of the school's ICT facilities.

F. Pupil-Friendly Summary

At Singlewell Primary, our ICT is here to help you learn and communicate safely. You must not:

- Bully or be unkind online.
- Share rude, offensive, or harmful material.
- Share nude or semi-nude images or videos.

Approved: _____

- Use ICT for illegal activities or to break rules.
- Access sites, programs, or devices without permission.
- Damage ICT equipment or try to hack systems.

Always ask for help if you are unsure, and use ICT responsibly to learn, create, and work safely.

4.1 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's behaviour policy.

5. Staff (including governors, volunteers, and contractors)

5.1 Access and Equipment

- The school's Business Manager/ICT Manager manages access to the school's ICT facilities and materials for school staff.
- Staff are provided with unique accounts and passwords to access school ICT facilities.
- School-issued devices remain the property of the school and must be used primarily for school purposes.
- Staff must store devices securely, use strong passwords, and follow data protection guidelines.
- Any loss, theft, damage, or compromise of school equipment must be reported immediately.

5.2 Email and Phones

- The school provides each member of staff with an email address.
- School email accounts and phones are for work purposes only.
- Staff must not share personal emails or phone numbers with pupils or parents.
- Sensitive information must be sent securely. Staff must follow data protection procedures if emails are sent in error.
- Any recording of phone calls must comply with the school's protocols (CPOMS).

5.3 Personal Use

- Occasional personal use of school ICT is permitted, as long as it does not interfere with work, pupils' learning, or constitute unacceptable use. Internet history must be deleted regularly and personal information must not be stored on school devices.
- Staff must not store school data on personal devices.
- Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Approved: _____

- Personal social media use must remain professional and follow school guidelines.

5.4 Remote Access

- Remote access is allowed only via approved and secure methods.
- Staff must follow the same rules and guidelines when accessing school ICT offsite.

5.5 School Website

- Only authorised staff may manage official school websites.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not appear anywhere on the website, particularly in association with photographs.
- Updates and content uploaded must comply with school guidelines at all times.

5.6 Monitoring and Filtering

- The school may monitor and filter ICT use to safeguard pupils, ensure legal compliance, and maintain effective operations.
- The school uses Primary technologies to ensure robust filtering and monitoring occurs on all ICT devices.
- Staff are informed of monitoring systems and must follow associated policies.
- Concerns about monitored activity should be raised with the DSL.

6. Pupils

6.1 Access to ICT facilities

- Computers, tablets, and other equipment are available to pupils only under the supervision of staff, in the ICT suite or classrooms.
- Pupils have individual logins for educational platforms such as Purple Mash, Times Table Rock Stars, and EdShed. Pupils must not share their login or password with other pupils; only school staff or trusted adults at home may know them.
- Email communication between pupils can be set up via Purple Mash for educational purposes (e.g., class communication activities). All messages must be approved by the class teacher to ensure they are appropriate, respectful, and safe.
- Pupils must immediately tell a teacher they view or receive any inappropriate use of ICT or the internet.

6.2 Unacceptable Use of ICT and the Internet Outside School

Pupils may be sanctioned under the school's Behaviour Policy if they use ICT or the internet in a way that is unsafe, illegal, or against school rules, even when not on school premises. This includes:

- Being unkind or bullying online — including messages, emails, or images.
- Sharing or looking at harmful or inappropriate material.
- Sharing personal information about themselves, other pupils, or staff without permission.
- Saying things online that could hurt the school's reputation or upset others.
- Trying to access files, systems, or areas they are not allowed to.
- Helping others break the rules or access school ICT without permission.
- Damaging school computers, tablets, or other devices.
- Using someone else's account or password without permission.
- Using rude or offensive language online.
- Doing anything illegal online, such as hacking, downloading unsafe material, or breaking copyright rules.

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course. However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the school's facilities at the head teacher's discretion.
Where parents/carers are granted access in this way, they must abide by this policy.

8. Data Security

The school is responsible for keeping its computers, devices, systems, and information safe. This includes protecting staff, pupils, and other users, and following the latest guidance on cyber safety. Everyone using the school's ICT facilities should use safe computing practices at all times.

We protect our systems using:

- Firewalls and security features
- User logins and multi-factor authentication
- Anti-virus and anti-malware software
- Regular software and security updates

8.1 Passwords

- Use strong passwords and keep them secret.
- Staff change passwords when prompted or required to ensure they stay protected.

8.2 Software and Updates

- School devices have regular updates and anti-virus protection.
- Software or files are not deleted without permission.

Approved: _____

- Files from outside must be checked before opening.

8.3 Data Protection

- All personal data must be stored safely and used according to the school's Data Protection Policy.
- Staff must not take or share school or pupil data without permission.

8.4 Access and Encryption

- The school makes sure that its devices and systems have an appropriate level of encryption.
- Everyone has clear access rights; people do not access things they are not allowed to.
- Devices are Logged out of or locked when not in use.

9. Using the Internet safely and effectively

The Internet is an important part of learning and school life and the school's wireless internet connection is secure. It helps pupils explore, supports teachers in their work, and improves school administration. Pupils who use it responsibly are entitled to access it.

9.1 Purpose and Benefits

- The Internet is used to support teaching and learning, develop ICT skills, and provide access to educational resources worldwide.
- Pupils can communicate safely with others for learning purposes and access expert advice.
- Staff can use the Internet to access professional development and share good practice.
- Pupils and staff have access to the school's Wi-Fi across the premises to support learning and school activities.
- Carefully planned use of ICT can also help reduce workload and support learning with age-appropriate tools.

9.2 Supervised Access for Pupils

- Internet access is **age-appropriate and filtered.**
- **Key Stage 1:** Pupils use the Internet with adult guidance, and for supervised activities.
- **Key Stage 2:** Pupils use the Internet across the curriculum and approved class email accounts under supervision.
- Pupils must ask permission before using the Internet and follow staff instructions.
- Parents must give written consent for their child to access the Internet at school via Admicity.

9.3 Safe and Responsible Use

- Pupils must only use approved websites and resources.
- Personal information, passwords, and contact details must never be shared.
- Pupils must tell a teacher immediately if they see anything that makes them uncomfortable or upset.

Approved: _____

- Email and online communication should always be polite, respectful, and for learning purposes only.
- Pupils are taught to check information carefully, think critically, and evaluate online content.

9.4 Monitoring and Security

- All Internet use is monitored using Primary Technologies to keep pupils and staff safe and ensure compliance with school rules.
- The school works with parents, the local authority, and the Internet provider to maintain safe and secure access.
- Despite filtering, pupils may occasionally see unsuitable material; staff will take immediate action if this happens.

9.5 Parental Guidance

- Parents are encouraged to monitor their child's Internet use at home and discuss safe and responsible online behaviour.
- Regular informative computing updates are sent home (within the newsletter) to support parents understanding of how children should be using technology (including the internet) in a safe, responsibly and appropriate way.

10. Social Media

Social media is an established part today's society, connecting people around the world for communication, learning, and sharing information. While it offers many opportunities, it also brings risks that require all members of the school community to use it safely, responsibly, and respectfully.

10.1 Staff

- Staff must maintain professional standards online and never share content that could harm the school's reputation or the wellbeing of pupils and colleagues.
- Staff should not contact pupils or parents via personal social media accounts. Where a personal relationship existed prior to employment at the school, staff are expected to maintain appropriate professional boundaries and must not engage in any school-related communication via personal social media platforms.
- Any concerns about online activity involving staff or pupils should be reported to the Head teacher or Designated Safeguarding Lead (DSL).

10.2 Pupils

- Pupils will not access social media in school, unless it is part of a curriculum activity
- Pupils should only use social media in a safe and responsible way, in line with this policy's rules and guidelines.
- Pupils must never share personal information, passwords, or images online without permission from a trusted adult.
- Pupils must tell a teacher immediately if they see anything online that is inappropriate, upsetting, or makes them feel unsafe.
- Pupils are not allowed to access public or unregulated social media accounts during school hours.

Approved: _____

- Pupils are aware that most social media platforms such as Instagram, TikTok and Snapchat have a minimum age rating of 13. Therefore, pupils should not set up or use personal social media accounts.

10.3 Parents/Carers

Instagram 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.

Parents/Carers will:

- Monitor their child's social media use at home and talk to them about safe online behaviour.
- Set appropriate privacy settings and guide their children on what is safe to share online.
- Share with the school any concerns about pupils' social media use that could affect their safety or wellbeing
- Respect staff privacy and professional boundaries; they must not attempt to contact staff via personal social media accounts regarding school matters.

11.Policy Access

11.1 Pupils

- Posters with rules for safe and acceptable ICT and internet use will be posted in all rooms where computing devices are used.
- Pupils will be informed the internet use will be monitored. Instruction in responsible and safe use should precede Internet access.

11.2 Staff

- All staff must accept the term of the 'Responsible ICT and Internet Use' statement before using any computing resource in the school.
- All stakeholders including teachers, governors and support staff will be provided with a copy of this policy and the importance will be explained.

12. Monitoring and review

The head teacher will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board are responsible for reviewing and approving this policy.

Approved: _____

13. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff code of conduct
- Data protection
- Remote Learning and Acceptable Use of Technology Policy
- Computing Policy

Approved: _____

Appendix 1

EYFS/KS1 Rules for responsible ICT and Internet Use

These rules help keep everyone safe and kind.

- I will ask an adult before I use a computer, tablet, or the Internet. 
- I will use my own login and keep it secret.
- I will only look at my own work.
- I will be kind and polite when I use technology 
- I will only click on things my teacher shows me.
- I will never share my name, address, phone number, or passwords. 
- I will not send messages unless a teacher helps me.
- I will tell an adult straight away if I see something that makes me feel sad, worried, or scared.
- I know that adults help keep me safe when I use 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: _____

Appendix 2:

KS2 Rules for responsible ICT and Internet Use

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

- I will ask permission before using ICT devices or going online.
- I will use only my own login and password and keep them secret.
- I will only open, change, or delete my own files and work.
- I will not bring software, memory sticks, or other digital devices into school without permission.
- I will only email or message people my teacher has approved.
- The messages I send will be polite, sensible, and respectful.
- I will never share personal information, such as my home address, phone number, or passwords, or arrange to meet someone online.
- I will ask a teacher before opening an email, message, or attachment from someone I do not know.
- I will not use chat rooms or messaging services unless a teacher has said it is allowed.
- If I see or receive anything that makes me feel unhappy, worried, or uncomfortable, I will tell a teacher straight away.
- I understand that the school may check my use of ICT devices and the websites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use ICT devices or the Internet at school.

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: _____

Appendix 3:

Acceptable Use Policy 2026

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 a combination of numbers, letters and symbols, with 8 or more characters, may 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 2018 and UK GDPR. 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 R Catt and/or the Online Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead Mrs R Catt/or the Online Safety Coordinator 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 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.

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.

Approved: _____

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 and/or the Online Safety Coordinator 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.

23. I will not I will maintain professional standards online and will not contact pupils via personal social media accounts. I will ensure that my use of social media, messaging, and communication apps aligns with the school's AUP, professional expectations, and safeguarding requirements.

24. I will use AI and new technologies only in line with the school's AI guidance and curriculum policies. I will ensure that any AI or online tools used do not compromise pupil safety, privacy, or professional standards.

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.....

Approved: _____

Appendix 4:

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 or Designated Safeguarding Lead Mrs R Catt.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer practise with Technology" are available to help you consider how to protect yourself online. Please 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 or the Designated Safeguarding Lead if you have any queries or concerns regarding this.

Yours sincerely

Mrs R Catt
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: _____