Pupil and Staff Acceptable Use Policies

Date reviewed: September 2022 **Next review: September 2023**

Kent County Council Online safety (e-Safety) Strategy Group

Introduction:

This policy details Acceptable Use Policies for pupil and staff users of school information systems at Clarendon Infant School. It has been adapted from the Kent County Council Acceptable Use Policies, as recommended by Wiltshire County Council.

Purpose:

We believe that Acceptable Use Policies should not be used to limit the ways in which children and adults use technology, but should aim to ensure that the children and adults are protected and are educated about safe and appropriate online behavior.

Children and young people should be empowered and supported to take responsibility for their own use of technology. With internet use an essential feature of children's everyday life, it is important that the Pupil Acceptable Use Policy is supported with regular, embedded and progressive education for children, which clearly highlights safe and positive online behavior that is appropriate to their age and agility.

All children and staff who use ICT must be aware of the school expectations whether on or off site.

Contents:

Clarendon Infant School - Pupil Acceptable Use Policy

The Pupil Acceptable Use Policy and Computing Rules should be discussed with children on a regular basis as well as when they are actually using technology. Pupils must be made aware that their internet and technology use may be recorded or monitored for safety and security reasons prior to internet or technology access. We understand that it is unlikely that all children will be able to 'sign' or give informed consent to an Acceptable Use Policy, however it is important that children are involved as much as possible in this process, as online safety education begins as soon as children being using technology.

As part of their computing and online safety education, children will be taught to:

- only click on links and buttons when they know what to do
- keep their personal information and passwords safe online
- only send messages online which are polite and friendly
- know the school can see what they are doing online
- not to bring their own devices into school
- know that if they do not follow the rules then they will be given sanctions as detailed in the Behaviour Policy (eg think, time out) and ultimately access to computing equipment/internet use may be withdrawn.
- always tell an adult/teacher if they see something online makes them feel unhappy or worried

Computing Rules will be displayed in each classroom and shared with the children on a regular basis. These rules will be shared with parents and parental agreement sought prior to any internet use.

Clarendon Infants' School
Ordnance Road, Tidworth
Hampshire, SP9 7QD
Tel 01980 843 381
Fax 01980 847 877

Headteacher Mrs Karen Ward

Dear Parent/Carer,

At Clarendon Infant School all pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to:

- computers, laptops and other digital devices such as iPads
- the internet, which may include search engines and educational websites
- digital cameras, web cams and video cameras
- voice recorders

Clarendon Infant School recognise the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety policies and procedures alongside the school's safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. Our internet access has built in filtering managed by Oakford Internet Services and Netsweeper that restricts access to sites containing inappropriate content. However no system can be guaranteed to be 100% safe. The school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the school's internet and ICT facilities.

At Clarendon Infant School we expect all pupils to be responsible for their own behaviour when using technology and accessing the internet. Please read the attached Pupil Acceptable Use Policy with your child and sign and return the permission form so that your child may use the internet at school. We understand that your child may be too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision making process and believe a shared commitment is the most successful way to achieve this.

For more information please view our Online Safety Policy which is available on the school website.

Yours sincerely,

K A Ward

Karen Ward
Executive Headteacher

Pupil Acceptable Use Policy

Parent/Carer Permission Form

I, with my child, have read and discussed the Clarendon Infant School Pupil Acceptable Use Policy and Computing Rules.

As parent/carer of the named pupil, I give permission for my child to have access to the internet and computing systems at Clarendon Infant School.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons to safeguard both my child and the school's systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

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

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the school online safety approaches and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name……Signed (if appropriate)……..

Class…… Date……..…..

Parent's Name……..Parent's Signature…….

Clarendon Infant School – Staff Acceptable Use Policy

The Staff Acceptable Use Policy puts in place clear boundaries for all members of staff regardless of their role. This will apply to the whole staff group, including teaching and non-teaching staff, volunteers (including governors) and external contractors (e.g. supply teachers).

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 ICT includes 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 understand that insurance cover provides protection for school owned devices from the standard risks whilst the device is on site or in my home but excludes theft from a car or other establishment. Should the device be left unattended and is stolen, I will be responsible for its replacement.

5. 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.

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

7. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and the General Data Protection Regulations (GDPR) 2018. 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 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.

8. I understand that best practice is to use a school device (laptop or iPad) when offsite to check school emails. Where this is not possible, the use of a personal device is permitted. I understand the email account must not be set up permanently on any personal device using an app and must only be accessed via Office365 online. The password must not be stored on the device. I will not keep 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, mobile phones).

9. 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.

10. I will respect copyright and intellectual property rights.

11. I have read and understood the school's Online Safety Policy.

12. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Designated Safeguarding Lead/Online Safety Lead (headteacher).

13. I will report any data breach to the Data Protection Officer in line with the school's procedure for reporting such events. I will adhere to the practice and principles of the General Data Protection Regulations (2018) and support the school in its efforts to be compliant.

14. 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 (Liz Howe) or our IT support, Oakford Technology (01980 888088), as soon as possible.

15. 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 with these external bodies will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal communication channels e.g. personal email or social networking. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher. Communication between staff, for example, to report absence, can be made using personal communication devices.

16. I will ensure that my online reputation and use of ICT 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, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school Acceptable Use Policy, Code of Conduct and the Law.

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

18. 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.

19. If I have any queries or questions regarding safe and professional practice online either in school or offsite, then I will raise them with the Designated Safeguarding Lead/Online Safety Lead (headteacher) or Computing Lead (Liz Howe).

Policy Breaches or Concerns

20. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school Online Safety and Child Protection Policies.

21. I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the allegations against staff policy.

22. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct.

23. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct

24. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I understand that my use of the school information systems (including any devices provided by the school), school internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation. Where it believes unauthorised and/or inappropriate use of the school's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure.

I have read, understood and agree to comply with the Clarendon Infant School Staff Acceptable Use Policy when using the internet and other associated technologies, both on and off site.

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

Accepted by: ……Print Name: ……

Clarendon Infant School - Wi-Fi Acceptable Use Policy
(For visitors using school Wi-Fi)

This is not an exhaustive list and all visitors are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the law.

The school can provide Wi-Fi for school visitors when appropriate and allows access for education use onsite only via Captive Portal monitoring Wi-Fi.

1. The use of ICT devices falls under Clarendon Infant School Staff Acceptable Use Policy, Online Safety Policy, GDPR Policy and Safeguarding & Child Protection Policy which all students, visitors and volunteers must agree to, and comply with.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. Clarendon Infant School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the school premises that is not the property of the school.

3. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

4. School owned information systems, including Wi-Fi, must be used lawfully and 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.

5. I will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure (such as up-to-date anti-virus software, systems updates).

6. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

7. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

8. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

9. I will respect system security and I will not disclose any password or security information that is given to me. 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.

10. I will not attempt to bypass any of the school's security and filtering systems or download any unauthorised software or applications.

11. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the law including copyright and intellectual property rights. This includes the use of

email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead/the Online Safety Lead (headteacher) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Designated Safeguarding Lead/Online Safety Lead (headteacher).

15. I understand that my use of the school's Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes, then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Clarendon Infant School Wi-Fi Acceptable Use Policy.

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

Accepted by: ……. Print Name: …….

Clarendon Infant School – Official Social Networking Acceptable Use Policy for use with staff running official social media accounts

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety. I am aware that the tool (e.g. Facebook, Twitter) is a public and global communication tool and that any content posted may reflect on the school, its reputation and services.

2. I will not use the site/page/group to express any personal opinions or 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 the school into disrepute.

3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (headteacher). The headteacher retains the right to remove or approve content posted on behalf of the school.

4. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

5. I will follow the school's policy regarding confidentiality and data protection/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school via school owned devices. Images taken for the sole purpose of inclusion on social media will not be forwarded to any other person or organisation.

6. I will promote online safety in the use of social media and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by the Designated Safeguarding Lead (headteacher) prior to use.

7. I will set up a specific account/profile using a school provided email address to administrate the account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses will not be used. The school Designated Safeguarding Lead (headteacher) will have full admin rights to the site/page/group.

8. Where it believes unauthorised and/or inappropriate use of the site/page/group or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

9. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead (headteacher) urgently.

11. I will ensure that the site/page/group is moderated on a regular basis as agreed with the Designated Safeguarding Lead (headteacher).

12. I have read and understood the school Online Safety policy and Social Media policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.

13. If I have any queries or questions regarding safe and acceptable practice online I will raise them with the Designated Safeguarding Lead (headteacher).

Policy Compliance, Breaches or Concerns

14. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

15.I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead in line with the school Online Safety and Child Protection Policies

16.I will report concerns about the welfare, safety or behaviour of staff to the headteacher, in line with the allegations against staff policy.

17.I understand that if the school believes that if unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

18.I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agree to comply with Clarendon Infant School Official Social Networking Acceptable Use Policy for Staff.

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

Accepted by: ……. Print Name: ……..