Clewer Green CE Aided First School
Hatch Lane, Windsor, SL4 3RL Tel: 01753 864544 Email: office@clewergreen.org.uk
Headteacher: Mr M Tinsley

'Inspiring Children'

Vision: Every child has been blessed by God with unique potential. Our vision for Clewer Green is to inspire and nurture children in a safe, happy and caring Christian community, where everyone is valued and enjoys learning.

'I can do all things through him who strengthens me'

Philippians 4:13

Safeguarding E-Safety Policy

THIS POLICY **MUST** BE READ IN CONJUNCTION WITH OUR **ACCEPTABLE USE POLICY**, OUR **CHILD PROTECTION POLICY** and our **SAFEGUARDING – CHILD PROTECTION COVID-19 ADDENDUM**

Aim

The Headteacher and Governing Board have a legal responsibility to safeguard children and staff and this includes online activity.

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our School Policy has been agreed by the Senior Leadership Team and approved by Governors and other stakeholders such as the Friends of Clewer Green.
- The School has appointed a member of the Governing Board to take lead responsibility for e-Safety.

The School e-Safety Coordinator is Mr Martin Tinsley.

Internet Content

How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

The following statements require adaptation according to the pupils' age:

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

The content of websites which the children and parents are signposted to for Home Learning are checked by our staff, although only recommended educational sights are used. Parents are asked to help and supervise their child's home learning if they are isolating due to Covid and be vigilant of the websites that their child is using.

Managing Information Systems

How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue which cannot be dealt with adequately within this document.

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

Broadband firewalls are configured to prevent unauthorised access between schools.

The Schools Broadband network is protected by a cluster of high performance firewalls and managed by Key Network Solutions (KNS).

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Portable media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

The implications of email use for the school and pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible. In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.

- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.

Can pupils' images or work be published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Images of a pupil should not be published without the parent's or carer's written permission.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School follows RBWM guidance regarding the use of photographic images of children.

How will social networking, social media and personal publishing be managed?

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the school community. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- Dynamic content filtering examines web page content or email for unsuitable words.
- URL monitoring records the Internet sites visited by individual users. Reports can regularly be produced to investigate pupil access.

Occasionally mistakes may happen and inappropriate content may be accessed. It is therefore important that children should always be supervised when using internet access and that Acceptable Use Policies are in place.
In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online. There is also an Incident Log Book kept in the ICT Suite to report breaches of filtering or inappropriate content being accessed. Any material that the school believes is illegal must be reported to appropriate agencies such as Thames Valley Police or CEOP.

Websites which schools believe should be blocked centrally should be reported to KNS. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc. just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

- The school will work with the KNS team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Thames Valley Police or CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How are emerging technologies managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within school systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to - but if inappropriately used, a video link could reveal security details.

Schools should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies. For instance text messaging via

mobile phones is a frequent activity for many pupils and families; this could be used to communicate a pupil's absence or send reminders for upcoming events.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's Safeguarding suite of policies (Child Protection, Positive Relationships and Behaviour, Peer on Peer Abuse and/or Anti Bullying).

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use or Mobile Phone Policy.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully,
- Processed for specified purposes,
- Adequate, relevant and not excessive,
- Accurate and up-to-date,
- Held no longer than is necessary,
- Processed in line with individual's rights,
- Kept secure,
- Transferred only to other countries with suitable security measures.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

How will Internet access be authorised?

Normally most pupils will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission should be encouraged for Internet access in all cases — a task that may be best organised annually when pupils' home details are checked and as new pupils join or as part of the Home-School agreement. If schools do request parental consent for internet access it is essential to record this data. Schools must be aware that students should not be prevented from accessing the internet unless the parents have specifically denied permission or the child is subject to a sanction as part of the school behaviour policy.

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.

- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

According to Setting Type

- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from inappropriate Internet use. The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Thames Valley Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to any incidents of concern?

e-Safety risks can be experienced unintentionally or deliberately by people acting inappropriately or even illegally. Any potential concerns must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported.

Staff should also help develop a safe culture by observing each other's behaviour online and discussing together any potential concerns. Incidents of concern may include unconsidered jokes and comments or inappropriate actions. Any illegal activity would need to be reported to the school Designated Safeguarding Lead.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the MASH or Local Authority e-Safety Officer if the offence is deemed to be out of the remit of the school to deal with.

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief and identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the MASH Team or e-Safety Officer and escalate the concern to the Police

- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the LA e-Safety Officer to communicate to other schools in the area.

Parents, teachers and pupils should know how to use the school's complaints procedure. The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. e-Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

- Any complaint about staff misuse will be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the Thames Valley Police and/or the MASH to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café. Ideally, young people would encounter a consistent internet use policy wherever they are.

Regarding internet access in the community, there is a fine balance between ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Organisations are developing access appropriate to their own client groups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practice may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences could be worthwhile.

Sensitive handling of cultural aspects is important. For instance filtering software should work across community languages and may need to consider the pupils' cultural backgrounds.

- The school will liaise with local organisations to establish a common approach to e– Safety.
- The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously

safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006 states that:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents
- Headteachers have the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed they should seek assistance from the police.

The DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Safeguarding Policies. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

How will mobile phones and personal devices be managed?

The Governors of Clewer Green CE Aided First School have decided that it is not appropriate for our children to bring mobile phones in to school. When a child has been found with a mobile phone or other personal device on their person, the phone or device will be removed and kept in the office. It can then be collected at the end of the day.

Communication of this Policy

How will the policy be introduced to pupils?

Many pupils are very familiar with culture of mobile and Internet use and it is wise to involve them in designing the School e–Safety Policy, possibly through a student council. As pupils' perceptions of the risks will vary; the e–Safety rules may need to be explained or discussed.

Clewer Green CE Aided First School has produced posters covering e–Safety rules which are available to display in every room with a computer to remind pupils of the e–Safety rules at the point of use. Consideration must be given as to the curriculum place for teaching e–Safety. This could be as an ICT

lesson activity, part of the pastoral programme or part of every subject whenever pupils are using the internet.

All users will be informed that network and Internet use will be monitored. An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. Pupil instruction regarding responsible and safe use will precede Internet access. e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas. Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods.

Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

All staff must understand that the rules for information systems misuse for Clewer Green CE Aided First School employees are specific and that instances of abuse of these systems will result in disciplinary procedures and potentially dismissal. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.
ICT use is widespread and all staff including administration, midday supervisors, caretakers, governors and volunteers should be included in awareness raising and training. Induction of new staff should include a discussion about the school e–Safety Policy.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user and that therefore discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- KNS who manage our filtering systems or any staff who monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom and these tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The school may be able to help parents plan appropriate, supervised use of the Internet at home and educate them about the risks. Parents should also be advised to check whether their child's use elsewhere in the community is covered by an appropriate use policy.

One strategy is to help parents to understand more about ICT, by running courses and parent awareness sessions.

- Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to read and sign the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats. Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Created:	May 2017
Reviewed:	September 2021
Next Review:	September 2022

Sarah Langley, Chair of Governors