e-Safety Policy
(including Mobile Devices Policy)

The purpose of the e-Safety policy.
The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-Safety. The policy relates to other policies including ICT curriculum, Internet Access, Bullying, Child Protection and Health and Safety.

Writing and reviewing the e-Safety policy
The school e-Safety Coordinator who will work closely with the Designated Safeguarding Lead as the roles overlap.

The e-Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is important?
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. However in line with LA policy we will not “over filter” as this creates an unnatural Internet environment which is not mirrored by access outside of school. In this, it is more important to educate rather than totally block. It is important for parents to understand this policy.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access
Information system security
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail content and the school web site
- Pupils may only use approved email accounts in the school (currently list is under development by the Local Authority).
- The contact details on the Web site should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The official school Twitter feed will also be displayed on the homepage.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work
- Photographs that include pupils will be selected carefully and will not compromise child safety.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers is obtaining in the home / school agreement for the publishing of pupil photographs on the website.
- Pupil's work can only be published on the school website unless the parent/carer has refused permission of the pupil and parents.

Social networking and personal publishing
The school will deny access to social networking sites in school for both pupils and staff. Twitter is permitted on some devices operated by senior members of staff in school and this will be limited to the official school feed @claregatepri. YouTube material can be viewed on staff laptops. Its use should be used with caution and staff should check material carefully before using in class.

Managing filtering
- The school will work with the LA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co-ordinator who will liaise with the Local Authority.

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

Assessing risks
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Handling e-Safety complaints
- The Headteacher / Deputy Headteacher will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding Procedures.

Community use of the Internet
All use of the school internet connection by community and other organisations shall be in accordance with the e-Safety policy.

Introducing the e-Safety policy to pupils
- E-Safety rules will be discussed with the pupils at the start of each year and reiterated as the year progresses.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- The children receive e-Safety lessons and are constantly reminded of online safety.
- All pupils in Key Stage 1 and 2 will sign an acceptable use agreement.

Staff and the e-Safety policy
- All staff will have access to the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic could be monitored.
- All staff have a professional email address provided by the school using the format aother@claregateprimaryschoool.co.uk. This address should be used for all emails of a professional nature. Staff email addresses must not be communicated to parents and staff should not enter into email conversations with parents / carers or pupils. All email contact between members of staff and parents / carers should be via the main school email address claregateprimaryschool@wolverhampton.gov.uk. This address is secure and must be used for the communication of personal data.
- Staff should exercise caution about material that is posted on social media sites. No school related posts should be made on personal social media accounts and feeds.

Discretion and professional conduct is essential.

Mobile Technology
- We do not allow pupils to bring their own mobile devices into school, or on trips in any circumstances and we will resist any parental pressure to break this rule.
- We also do not allow mobile devices to be kept in bags for use after school. The safety benefits are outweighed by the dangers of bullying and theft.
- If we know of a mobile device in school it will be confiscated and the parent requested to collect it. We take no responsibility for these devices and any child or family who breaks this rule will receive no help in retrieving or finding lost or stolen devices.
- School mobile technology will not be allowed to be in use at large around the school. They are for use in lessons only where pupil activity is monitored.
- In lessons children can be instructed to email, surf the Internet message or take photographs. Many of these activities form part of the curriculum.
- Children may not do this unless it is in lessons or supervised as part of a lunchtime break.
- Only apps downloaded by the school staff or technician will appear on school owned devices.
- The same rules of acceptable Internet use apply to mobile devices.
- Any text message that comes to our attention and is considered abusive or derogatory will be dealt with as part of our disciplinary policy. Parents / carers will be informed and if it is a completely out of school incident with no links to school advice will be given on how to deal with this themselves.
- No item of personal belonging is insured by us.
- We will teach the children the dangers of mobile devices.
- If the school suspects that there is abusive illegal material that device will be confiscated and the content investigated by the police. We may occasionally ask permission for a

parent / carer to disclose content as evidence so that disciplinary or police investigation can ensue.

Staff and Mobile Technology

- We do allow staff to have mobile devices on site and to keep them switched on for family emergency messages.
- All mobile devices should have a secure password or block, so if lost, personal information cannot be accessed by children. No mobile device brought in should have any image or content on it that if read or seen could bring that teacher into breach of duty. If devices have any such content they should not be brought in.
- Staff should not allow children to view their personal mobile device. It is too easy to receive a live text which pops up, that is not intended for children.
- Except in extreme emergency, these devices should not be used in teaching time. The Headteacher of Deputy Headteacher must give express permission to monitor devices in times of emergency.
- Personal devices should not be used for taking images of children. Official school devices should be used for this purpose. There should be no personal device or personal cloud storage of any images of children.
- Particular care should be taken when using mobile technology when children are getting changed. This could be construed as taking photographs and leaves the member of staff open to accusation.
- Staff can use personal mobile devices for contacting the school if off site.
- Staff must follow our code of conduct in relation to text messages. It is too easy to behave in a non-professional way because of the informality of the genre.

Visitors and Mobile Technology

- Are required to follow the same rules as staff except during performances when they are allowed to take photographs and video recordings as long as these are for personal use only.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, and conversations.

If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

It is intended that this policy be reviewed annually.

D J Saunders
Deputy Headteacher