

Claregate Primary School

e-Safety Policy and Acceptable Use Agreements



Mr D J Saunders
e-Safety Co-ordinator

Claregate Primary School e-Safety

FOREWORD

Taken from Wolverhampton LA e-Safety statement.

By placing children young people and families at the heart of the e-strategy, we recognise that learners must have the skills to keep themselves safe in the digital world. This follows the main educational recommendations of the Byron Report (2008) which advises that :-

- ***“In all schools, action is taken at a whole-school level to ensure that e-safety is mainstreamed throughout the school’s teaching, learning and other practices.”***
- ***“100% of schools should have Acceptable Use Policies that are regularly reviewed, monitored and agreed with parents and students.”***

As part of the five outcomes of the ECM agenda, it is not sufficient for them just to be safe, but they need to be e-confident, in order for them to:-

- enjoy and achieve
- stay safe
- be healthy
- make a positive contribution
- achieve economic well-being

At Claregate Primary School there are three approaches to achieving e-safety:

1. Dealing with the “here and now”: informing and making staff, children, young people and their families aware of the benefits and also the potential dangers of working on-line.
2. Building learning opportunities to develop children and young people as safe and e-confident learners, enabling their families to understand and support them in this area of their lives.
3. Technical safeguards such as appropriate web filtering and levels of access

Wolverhampton Safeguarding Children Board (WSCB) works closely to coordinate approaches to e-Safety with Wolverhampton City departments and external agencies.

Claregate Primary School

e-SAFETY POLICY

Contents

Section 1 - Introduction:

- Roles and responsibilities**
- Writing and reviewing the e-Safety policy**
- e-Safety skills development for staff**
- e-Safety information for pupils and parents / carers**
- Community use of the Interact**

Section 2 - Teaching and Learning:

- Internet use will enhance learning**
- Pupils will be taught how to evaluate Internet content**

Section 3 - Managing Internet Access:

- Information system security**
- e-mail**
- Published content and the school Learning Platform**
- Publishing pupils' images and work**
- Photographs taken by parents / carers for personal use**
- Social networking and personal publishing**
- Managing filtering**
- Managing emerging technologies**
- Protecting personal data**

Section 4 - Policy Decisions

- Authorising Internet Access**
- Password security**
- Assessing risks**
- Handling e-Safety complaints**

Section 5 - Communications Policy

Introducing the e-Safety policy to pupils

Staff and the e-Safety policy

Section 6 - The Learning Platform (LPPlus)

Section 7 - Monitoring and Review

Appendices

Appendix 1 - Acceptable Use Agreement - Key Stage 1 Pupils

Appendix 2 - Acceptable Use Agreement - Key Stage 2 pupils

Appendix 3 - Acceptable Use Agreement - School Staff

Appendix 4- Staff Laptop Agreement

Appendix 5 - Wolverhampton LA Infrastructure Overview

Claregate Primary School

e-SAFETY POLICY

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our children with the skills to access life-long learning and employment.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Claregate Primary School we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school; (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones and portable media players, etc).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator (and e-Learning co-ordinator) in our school is **Mr D J Saunders** who has been designated this role as a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance.

The Head and e-Safety coordinator updates the Senior Leadership Team and Governors and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety policy

This policy, supported by the school's Acceptable Use Agreement for staff and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies including those for e-Learning, Home-school Agreements, Behaviour and Discipline, Health and Safety, Safeguarding, and PSHE policies including Anti-bullying.

Our e-Safety policy has been written by the school, in conjunction with advice from Wolverhampton LA and government sources. It has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually along with the whole school Safeguarding policy.

e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues through the coordinator at staff meetings .
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

e-Safety information for pupils and parents/carers

- Pupils from Years 1 - 6 are required to adhere to an Acceptable Use Agreement. This document is explained to pupils and is signed within school.
- A copy of the Acceptable Use Agreement for Key Stage 1 and 2 pupils is made available to all parents via the school website.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website or within any other electronic media form.
- The parent's area of the school website contains useful information on e-Safety.
- The school will send out relevant e-Safety information through newsletters and on the school website.

Community use of the Internet

- No external organisations make use of school ICT facilities.

2. Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- 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.

3. Managing Internet Access

Information system security

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed on all school computers and is updated regularly.
- Security strategies will be discussed with Wolverhampton LA as appropriate.
- No communications device, whether school provided or personally owned, may be used for bullying or harassment of others in any forms.
- No applications or services accessed by users may be used to bring the school, or its members into disrepute.
- All users have a duty to respect the technical safeguards that are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to protect their passwords and personal network logins, and should log off the network or lock computers when leaving workstations unattended.
- All users should understand that network activity and online communications are monitored, including personal and private communications made via the school network. The Headteacher and Deputy Headteacher receive real-time active keystroke incident reports.
- All users must take responsibility for reading and upholding the standards laid out in the policy.

e-mail

- Pupils may only use their school Learning Platform approved e-mail accounts (where issued) on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school Learning Platform

The school Learning Platform is hosted and maintained by Wolverhampton LA. The contact details on the school website are the school address, e-mail and telephone number. Staff or pupils' personal information will **not** be published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. This permission will be obtained from parents / carers via the signing of the Home / School Agreement.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the school website particularly in association with photographs.
- Photographs of individual pupils will not be permitted to be placed on class websites. Only pictures of groups or group activities will be permitted.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents / carers.

Photographs taken by parents/carers for personal use

In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites. Parents/ carers co-operation is actively encouraged in this matter.

Social networking and personal publishing

- The school will block / filter access to all social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites.

Managing filtering

- The school's broadband internet feed is filtered centrally by Wolverhampton LA e-Services
- Real time monitoring of all devices connected to the school network takes place. Violations and incidents are reported automatically to the Headteacher and Deputy Headteacher.
- The school will work with Wolverhampton LA, The Department for Education and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If pupils or staff discovers an unsuitable site, it must be reported to the Class Teacher, e-Safety Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- The use of portable media such as memory sticks and CD ROMs will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school.
- The sending of abusive or inappropriate text messages outside school is forbidden.
- Staff will use a school phone where contact with pupils is required (and not their own personal mobile).
- Staff mobiles are used as a primary means of communication between school and staff during an off-site visit. These details are logged in the off-site visit documentation which is completed before a visit takes place.
- Staff should not use personal mobile phones during designated teaching sessions.

Protecting personal data

The school will collect personal information about you fairly and will let you know how the school and Wolverhampton LA will use it. The school will use information about pupils to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school or Wolverhampton LA. For other members of the community the school will tell you in advance if it is necessary to pass the information on to anyone else other than the school and Wolverhampton LA.

The school will hold personal information on its systems for as long as you remain a member of the school community and remove it in the event of you leaving or until it is no longer required for the legitimate function of the school. We will ensure that all personal information supplied is held securely, in accordance with the policies and practices of Wolverhampton City Council and as defined by the Data Protection Act 1998 and current GDPR legislation.

You have the right to view the personal information that the school holds about you and to have any inaccuracies corrected.

4. Policy Decisions

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety Policy
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password security

- Adult users are provided with an individual network, and Learning Platform login username and password, which they are encouraged to change periodically.
- All pupils are provided with an individual network username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school computer network and School Information Management System (SIMS)

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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. Neither the school nor Wolverhampton City Council can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher / e-Safety coordinator and recorded in school incident log.
- 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.
- Pupils and parents will be informed of the complaints procedure.

5. Communications Policy

Introducing the e-Safety policy to pupils

- Pupils from Year 1 - 6 will undertake specific e-Safety tasks via specific materials.
- Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PSHE lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Any breaches of the e-Safety policy could result in disciplinary action being taken
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

6. The Learning Platform (School Website)

- All staff will be trained and given advice on how to effectively use the Learning Platform.
- Parents will be informed about what the Learning Platform is and how it can enhance the learning of each child. All children will be given training on how to effectively use the Learning Platform.
- Children may be given a username and password to access secure resources and facilities through the Learning Platform. Children will be allowed to choose their own password and taught to keep this secure.
- The Learning Platform will be regularly monitored for incidents of cyber-bullying, inappropriate use of language or the uploading of inappropriate files. Pupils will be informed that the sending of messages and emails through the Learning Platform is monitored and misuse of the messaging system will result firstly in a warning, followed by removal as a user of the Learning Platform should such behaviour be repeated.
- Children will be allowed to upload photographs of groups or group activities onto their homepage but not individual pictures of themselves.
- Class teachers will monitor the use of the Learning Platform. Any misuse of the Learning Platform will be reported to the e-Safety Co-ordinator / Headteacher.

7. Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-Safety Coordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety / e-Learning Coordinator, Designated Child Protection / Safeguarding Coordinator, and Governors with responsibility for e-Safety and Governors with responsibility for Child Protection. Ongoing incidents will be reported to the full governing body.

The e-Safety policy will be revised by the e-Safety Coordinator.

Claregate Primary School
e-SAFETY POLICY
Appendices

Appendix 1 - Acceptable Use Agreement - Key Stage 1 Pupils

Appendix 2 - Acceptable Use Agreement - Key Stage 2 pupils

Appendix 3 - Acceptable Use Agreement - School Staff

Appendix 4 - Staff Laptop Agreement

Appendix 5 - Wolverhampton LA Infrastructure

Claregate Primary School

e-Safety Acceptable Use Agreement

Key Stage 1 Pupils



When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- ☺ only share my password(s) with parents / carers and never with my friends or peers
- ☺ talk to my teacher before using anything on the internet
- ☺ only open pages which a responsible adult has said are OK
- ☺ tell a responsible adult if anything makes me feel scared or uncomfortable
- ☺ not give my mobile phone number to anyone who is not a friend in real life
- ☺ not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- ☺ not upload photographs of myself onto the internet
- ☺ never agree to meet anyone via the internet
- ☺ only communicate with people I know in real life
- ☺ tell my teacher if I get a nasty message through a computer or phone
- ☺ not reply to any nasty message or anything which makes me feel uncomfortable
- ☺ make sure all messages, e-mails and texts I send are polite
- ☺ only email people I know or if my teacher agrees
- ☺ only use my school email in school
- ☺ only put something on the Learning Platform that I would be happy to say to my teacher

I understand:

- ☺ Using computers and mobile phones safely and appropriately can make everyone's learning more enjoyable
- ☺ Anything I do on the computer may be seen by someone else
- ☺ Anything I put on the Learning Platform will have my name next to it

Claregate Primary School

e-Safety Acceptable Use Agreement

Key Stage 2 Pupils



When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- 😊 only share my password(s) with parents / carers and never with my friends or peers
- 😊 only visit sites which are appropriate to my work at the time.
- 😊 work only with individuals or groups agreed by my teacher or other responsible adult
- 😊 tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- 😊 make sure all messages, texts and e-mails I send are respectful
- 😊 inform a responsible adult if I get a nasty message, text or e-mail or get sent anything that makes me feel uncomfortable
- 😊 do not reply to or forward any nasty message or anything which makes me feel uncomfortable
- 😊 not give my mobile or home phone number to anyone who I don't know or have not met
- 😊 only email people I know or those approved by a responsible adult
- 😊 only use email in school which has been provided by school
- 😊 only connect to the agreed school wireless broadband while in school
- 😊 talk to a responsible adult before joining chat rooms or networking sites
- 😊 I will inform a responsible adult if I come across anything in chat rooms or networking sites that makes me feel uncomfortable
- 😊 Inform staff immediately if I suspect that anybody is using the internet inappropriately
- 😊 always keep my personal details private, things like my name, family information, my journey to school, my pets and hobbies are all examples of personal details
- 😊 always check with a responsible adult and my parents before I upload photographs of myself or anyone else
- 😊 never meet an online friend without taking a responsible adult that I know with me

I understand:

- 😊 Using computers and mobile phone safely can make everyone's learning more enjoyable
- 😊 Anything I do on the computer may be seen by someone else
- 😊 Anything I put on the Learning Platform will have my name next to it
- 😊 Most social networking sites have a minimum joining age and it is a criminal offence to give false information e.g. lie about my age or gender
- 😊 Not everyone on line is who they say they are

I know that once I post a message, picture or any other item on the internet then it is completely out of my control.

I know that anything I write or say or any website that I visit may be being viewed by a responsible adult

Claregate Primary School

e-Safety Acceptable Use Agreement



School Staff

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users while supporting learning.

I agree that I will:

- only use personal data securely
- implement the schools e-Learning and e-Safety policies
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts in school
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- only give access to appropriate users when working with blogs or wikis etc...
- **set strong passwords** – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the e-Safety Coordinator
- ensure that videoconferencing is supervised appropriately for the learner's age
- read and sign the acceptable use policy
- pass on any examples of Internet misuse to a senior member of staff
- post any supplied e-Safety guidance appropriately
- think carefully about what is stored on my laptop and make efforts to store sensitive data on the school server or private area on the Learning Platform

I agree that I will not visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children to danger
- any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Name Date

Claregate Primary School School Staff Laptop Agreement



This document is an agreement between both staff and school, and shall be binding for the duration of employment at the school.

General:

1. The laptop shall remain the property of the school.
2. The laptop shall be retained by staff in order to exercise their professional duties.
3. The laptop shall be returned to school upon a member of staff leaving
4. and any additional software/saved data removed.
5. Staff are to take proper care of the laptop at all times.
6. Staff shall be responsible for the security of the laptop, ensuring it is in a lockable cupboard when unattended in school and ensuring all reasonable precautions are taken when transporting the laptop.
7. Any additional software installed on the laptops is to be correctly licensed.
8. All faults are to be reported to the e-Learning Co-ordinator.

Usage:

1. The laptop shall be available for use in school as required.
2. Staff shall be aware of the issues relating to access to Internet sites not relevant or appropriate to their professional duties.
3. Staff shall operate Internet access with due regard to school and Wolverhampton City Council policies.
4. Staff shall use the laptop in a responsible and professional manner.
5. Staff will be expected to use the laptop for:
 - Planning
 - Delivery of lesson
 - Record Keeping
 - Analysis of assessment
 - Target Setting
 - Accessing Learning Platform
 - Report Writing
 - Other professional duties

The school agrees to provide training for teachers in order to make effective use of their laptop.

The following equipment has been provided by Claregate Primary School for staff use:

Make:	Model:	Serial Number:	Asset Tag No:

I _____ agree to the terms and conditions above.

Signed: _____ Date: _____

Signed on behalf of Claregate Primary School by:

Signed: _____ Position: _____

Name: _____ Date: _____