Claremont Community Primary School & Children's centre

e-safety Policy

Introduction

This e-safety Policy has been written by the school's Information Communication Technology Coordinator. It has been agreed by the Senior Leadership Team and approved by the Governing Body. The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan for and make use of ICT, for example, web-based resources and e-mail. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills in their use. Access to the Internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach towards its use.

Purpose

The purpose of internet access and the use of digital media devices in school are to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

This policy provides clarity on what is permitted and what is to be deemed as inappropriate internet and device usage and is pertinent to all children, all members of staff and any other adult working in school.

Audience

This policy document, having been presented to and agreed by the staff and the Governing Body is available for all individual members of staff and Governors. Copies are available for visiting teachers, outreach staff and parents.

(*An electronic copy is available on Google Drive- staff handbook and*[1] *the school blogsite)*

Benefits to the school of the use of the internet

There are a number of advantages to the school. These benefits include:

- Access to world-wide educational resources including museums and art galleries;
- Information and cultural exchanges between students world-wide;
- Use of the blog to share work and comment on each others work
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for pupils and staff;
- Staff professional development - access to educational materials and good curriculum practice;
- Communication with the advisory and support services, professional associations and colleagues;
- Exchange of curriculum and administration data with the LEA and DfEE.
- Access to learning for children whenever and wherever convenient.

Using the Internet to provide effective learning

Teachers, parents and pupils need to develop good practice in using the Internet as a tool for teaching and learning. We recognise that there is a fine balance between encouraging autonomous learning and maintaining adequate supervision and have the following systems to ensure Internet use is as safe as possible.

- Internet access is provided by the LEA. This includes filtering appropriate to the age of pupils;
- Internet access is planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement;
- Staff will select sites which will support the learning outcomes planned for pupils' age and maturity;
- Pupils will be educated in taking responsibility for internet access.
- Pupils will be given clear directives on times when it is acceptable to use the Internet for educational purposes and when it is not.

Planning and use of the Internet

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirement:

- Pupils will be given clear objectives for internet use.
- Staff will select sites which will support the learning outcomes planned for the pupils' age and maturity.
- Staff and pupils **will not** be allowed to access public chat rooms, including social network sites.
- Staff and pupils must not access inappropriate sites that could put others at risk.
- New facilities will be thoroughly tested before pupils are given access.

- At **Foundation Stage & Key Stage 1,** the majority of the access to the Internet will be by teacher or adult demonstration. However, there may be situations when pupils have supervised access to specific approved on-line materials.
- At **Key Stage 2**, internet access will be granted to individuals to use independently, either within the classroom or in the ICT rooms. Although working independently, pupils at all times will be under supervision by a teacher or adult employed by school.
- If staff or pupils discover unsuitable sites, the URL (address) and content will be immediately reported to the authority via the ICT Leader and in his/her absence the Headteacher or Deputy Headteacher.
- Staff will ensure that the use of internet derived materials by staff and pupils complies with copyright laws.

Teaching pupils to evaluate Internet content

Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher. This level of control is not so straightforward with internet-based materials. The approach to this problem is as follows:

- Pupils are taught ways to validate information before accepting that it is necessarily accurate;
- Pupils are taught to acknowledge the source of information, when using internet material for their own use;
- Pupils are made aware that the writer of an e-mail or the author of a web page might not be the person claimed;
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable;
- Pupils are encouraged to make an informed choice about their choice of reference material.

Use of digital and video images

Digital and video images have created significant benefits to learning. Staff and pupils must be aware of the risks associated with sharing images and videos over the internet.

- Photographs and videos of children are taken within the school environment and are used as a means of sharing and celebrating learning and achievement and are stored on the school network.
- Photographs that are published on the wblogsite will be carefully selected and will only be done so with the permission of their parents or carers.
- Written permission from parents / carers will be obtained as part of the admissions information and will be held in school. It is staff's responsibility to ensure that they follow these guidelines and do not

externally publish photos or videos of children without parental permission.

- If staff are completing work for external sources for their own CPD (e.g. research projects, management courses etc), staff must request parental permission outlining where and why the photo or video is being used.
- Photographs should be taken using school devices (e.g. cameras, netbooks, iPads). Photos should not be stored on personal devices (e.g. phones, iPods, laptops).

Managing e-mail

E-mail is an essential means of communication within education. At Claremont School we have a google drive domain that is set to ensure that only people with authorised accounts under claremontprimaryschool.co.uk can communicate via email with children's accounts. Each class has a class email that can be used for external reasons; this account is not openly accessible to children and should only be used under adult supervision – the password for this account is stored in the ICT handbook on google drive.

- All email communication is accessible by the domain administrator
- Pupils need to use e-mail as part of the National Curriculum 2000 Orders;
- Pupil e-mail can only be used in school for educational purposes;
- Pupils will not be allowed to access personal e-mail from the school system;
- Pupils may send a e-mails as part of planned lessons to others in the Claremont domain;
- Incoming class e-mail will be regarded as public;
  Messages sent using the school domain name are regarded in the same way as messages written on school headed paper;
- The forwarding of chain letters is banned;
- Staff will use personal e-mails responsibly to assist their role within school. When sending personal emails, staff must be vigilant not to place or leave e-mails on show to pupils. Personal email apps must not be added to any school device not password saved within the site.

Social Media

For the purposes of this policy, social media includes (but is not limited to) internet forums, blogs, wikis, podcasts, photograph websites (Flickr, Animoto etc), Facebook and Twitter. Staff should follow these guidelines in relation to any social media sites/apps that they use, both at work and in their personal lives.
This policy applies to all staff working at Claremont Community Primary School & Children's Centre. This includes all teachers, teaching assistants, dinner time staff, site staff, administrative staff, governors and volunteers. The reason for this policy is to protect the safety of staff and to assist those working with pupils to work safely

and responsibly. Furthermore, it sets out to offer a code of practice relevant to social media for professional and personal use.

- Staff should not access social media sites from the school's computers or other school device when working in school unless previously agreed and sanctioned by the Headteacher, and for educational purposes only.
- Staff should understand that anything they write (regardless of privacy settings) could be made public by other users. Staff should ensure they remain professional and ensure a clear distinction between professional and personal lives.
- Any use of social media should not:
    - Bring the school in to disrepute
    - Breach confidentiality
    - Breach copyrights
    - Bully, harass or discriminate
    - Be derogatory to others or about others
- The school appreciates that people will make use of social media in a personal capacity. Staff must be aware that if they are recognised from their profile as being associated with the school then certain opinions expressed could be considered to affect the reputation of the school.
- When using social media sites, staff should not share login or password details with others.
- If using social media sites/apps on personal phones, staff should ensure a lock/pin code is used to protect entry to the phone.
- Personal mobile and home numbers should be kept private.
- Staff should not make 'friends' of pupils at school. Staff should also think very carefully about communication via social media sites with parents and other family members of children in school as this leaves the member of staff open to the sharing of details and photographs.
- The use of Twitter for private use can be extremely beneficial for CPD purposes. Personal accounts must remain so and there must be an understanding that they will reflect upon a teacher's professionalism and therefore impact on a school's reputation. Staff should remember that nothing should be written that they would not mind repeating in front of a colleague, parent, Governor or Headteacher.

Managing the school website

Claremont has created a blogsite, which publishes pupils' work, promotes the school and provides information and resources for projects or homework. The blogsite reflects the school's ethos and information is accurate and well presented.

As the school's blogsite can be accessed by anyone on the Internet, the security of staff and pupils is considered carefully:

- The Headteacher delegates editorial responsibility of each class or subject site to a member of staff to ensure that content is accurate and quality of presentation is maintained;
- The blogsite complies with the school's guidelines for publications;
- The point of contact on the blogsite is the school address, telephone number and e-mail. Home information or individual e-mail identities are not published.

- Photographs/videos of pupils can only be used in any form with written permission from parents/carers pupils. First names only may be used with written permission.

Risk assessment

- Access to the internet from anywhere in school is done through the Blackpool Council intranet. Through this system firewalls are in place that should restrict access to certain sites. However, it is recognised that due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal.
- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks will be reviewed; Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken;
- The Headteacher will ensure that this policy is implemented effectively.
- All parents and children in school have signed to say they agree to work within the school safeguarding guidelines and policies when using the internet and understand that the school behaviour policy will be followed if he/she doesn't and his/her account may be frozen.

Neither the school nor Blackpool Borough Council can accept liability for the material accessed, or any consequences thereof.

Ensuring safe Internet access

- The LEA performs blocking and filtering;
- Pupils are informed that Internet use is supervised and monitored;
- The school works in partnership with the LEA and the DfEE to ensure systems to protect pupils are reviewed and improved;
- The ICT Team will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice;
- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the LEA via the ICT Team;
- Any material that the school suspects is illegal will be referred to the LEA;

Where minority languages are involved, appropriate measures will be used to ensure the process to select appropriate material is adequate.

Maintaining the security of school ICT system

- Security strategies are discussed with, and managed by, the LEA in conjunction with the IT company employed by school.
- The security of the whole system will be reviewed with regard to threats to security from Internet access;
- Virus protection is installed and updated regularly;
- Pupils and staff may not bring electronic storage devices into school.

Complaints regarding Internet use

Prompt action is taken if a complaint is made and is investigated thoroughly. See standard school complaints procedure for further details.Responsibility for handling incidents is given to a senior member of staff.

Consulting staff and pupils

- Rules for Internet access are posted near computer systems (see appendix);
- All staff are provided with the e-safety Policy, and its importance explained;

Parents' attention is drawn to the Policy on the school's blogsite.

Children's Rules for Responsible Internet Use

Copies of the Internet rules for pupils are displayed by all computers in the school. These rules are regularly brought to the attention of pupils.

*(**See Appendix A** for the Internet rules for pupils)*

Review

This policy was written by Miss Lisa Fleet, Information Communication Technology Coordinator and Assistant Headteacher to be shared with the Behaviour + Safety Governor committee on 12th May 2014.

Additional Information

Useful websites:

CEOPs e-safety site A site for children, parents and school staff	www.thinkuknow.co.uk
Government site for Parents (UK) Information about education for parents	www.dfee.gov.uk/parents/
Childnet – Know it all A site for primary school staff	www.childnet.com/resources/know-it-all-for-primary
NSPCC Keeping children safe online	www.nspcc.org.uk/internetsafety

Appendix A

Claremont Community Primary School & Children's Centre

Rules for Responsible Internet Use

The school has installed computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- **I will ask permission from a member of staff before using the Internet;**
- **I will use only my own login and password, which I will keep secret;**
- **I will not access other people's files;**
- **I will use the computers only for school work and homework;**
- **I will not use the netbook to access internet social chat sites;**
- **I will only send e-mails with my teacher's approval;**
- **The messages I send will be polite and sensible;**
- **I will not give my home address or phone number to anyone on the Internet;**
- **To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;**
- **I will only print out work with an adult's permission;**
- **I understand that the school may check my computer files and may monitor the Internet sites I visit.**

- **I understand that if I deliberately break these rules, I could be stopped from using the Internet, computers and other electronic media devices.**