ST. MARGARET'S ANFIELD CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety & Acceptable Use Policy

Reviewed January 2014

Introduction

Our vision for ICT is we use ICT creatively to enhance learning for all children as a tool to support all aspects of work in school.

We recognize the benefits of technology as an essential aspect of productive and social creative learning. We need to equip children with the skills and knowledge they need to use technology safely and responsibly and manage the risks, wherever and whenever they go online.

We understand our role as embedding a core of e-safety skills from an early age which will ultimately help protect children as they grow and mature regardless of how the technology and risks evolve. E-safety risks can be classified into content, contact and conduct and the risk element is often determined by the behaviour of the user rather than the technologies themselves.

An effective Acceptable Use Policy can help to establish, and reinforce safe and responsible online behaviour. This policy sets out to define what is meant by acceptable and inappropriate use of the Internet and to define the safeguards and sanctions put in place by the school.

Conditions of use for all users of the Internet at St Margaret's Anfield Church of England Primary School

It is expected that all users of the Internet, staff, pupils, students, parents and visitors be required to follow the conditions in the e-safety and Acceptable Use Policy.

- **No child may have unsupervised access to the Internet.**
- **Access should only be used through the user name and password, which should not be made available to any other person.**
- All Internet use should be **appropriate** to staff's professional work or the pupils' education.
- Use of the Internet and facilities such as the electronic email service are intended **for educational and administration purposes on**ly.
- **All users should show consideration** for other users both locally and with whom they may come into contact with on the Internet.
- A **responsible approach** to resources should be shown.

Procedures

- The school's ICT system will be reviewed regularly.
- Virus protection will be updated regularly.
- Acceptable use posters will be displayed to inform all users of ICT.
- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider (ISP) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be provided to the ISP via the ICT co-ordinators, the school Network Manager and the Headteacher.
- The school will take every reasonable precaution 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access.
- 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 and effective.
- E-safety education will be embedded within the curriculum.
- E-safety briefings and materials will regularly be made available to parents via school website and newsletters.
- Staff will always use a suitable and safe search engine when accessing the web with pupils.
- Staff, pupils and visitors should be aware that internet traffic can be monitored and traced to the individual user. **Discretion and professional conduct is essential.**
- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, eg (but not limited to) SMS text message, email, instant message or telephone or any other social networking media. Should special circumstances arise where such communication is felt to be necessary, the agreement of the Headteacher should be sought first and appropriate professional language should always be used.
- Staff must not use phones or personal mobile devices during teaching times.

"By Faith and Work"

Rules for Acceptable Use of ICT In School

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

- I will only access the system with my own login and password, which I will keep secret.
- I will not access other people's files.
- I will only use the computers for schoolwork and homework.
- I will not download and use material or copy and paste content which is copyright, (most sites will allow the use of published materials for educational use. Teachers will give guidelines on how and when pupils should use information from the internet.)
- I will not bring in memory sticks or disks from outside school unless I have been given permission. These can harm our system.
- I will ask permission from a member of staff before using the internet.
- I will only email people with my teacher's approval.
- The messages I send will be polite and responsible.
- I will not give out any personal details or arrange to meet people.
- If I receive any unpleasant materials or messages **at home** I will report these to my parent/carer and use the Report Abuse button.
- If I receive any unpleasant materials or messages at school I will report these to my teacher and use the Report Abuse button.
- I understand that the school will check computer files and monitor the internet sites visited by pupils and staff.

We encourage parents/carers to:

- Discuss e-safety issues with their children, supporting the school in its e-safety policy and reinforcing appropriate behaviour at home and in school.
- Liaise with the school if they suspect or have identified that their child is conducting risky behaviour online.
- Not allow their child to lie about their age and access social networking sites e.g. Facebook.
- Dissuade pupils from posting or uploading photographs /videos online.

Expectations of internet use at St Margaret's Anfield CE Primary School

- The school and governing body have adopted conditions for Internet use which are designed to maximize the use of the Internet as a learning resource and minimize unacceptable behaviour and access to unacceptable materials.
- All users have been made aware of the conditions of use.
- Parents and carers have been made aware of the conditions of use.
- All members of staff have been made aware of possible misuses of on-line access and their responsibility towards pupils.
- All pupils, staff and other users are required to follow the conditions laid down in the policy. **Any breach of these conditions may lead to withdrawal of internet access rights and could lead to disciplinary action and possible criminal prosecution**. In the case of employees breaching the conditions, this could lead to dismissal on the grounds of misconduct.
- Use of internet and e-mail facilities by pupils is intended for educational purpose only. It must be recognized that any view communicated over the internet may be deemed to be the view at the school/governing body and in some circumstances that of the LA. Any expressions of personal views must be cleared prior to endorsement to that effect.
- All users are responsible for good behaviour on the internet. Users are responsible for behaviour and communications over the internal network. It is assumed that all users will comply with established school standards.
- Users are responsible for all e-mail sent and for contacts made, that may result in e-mail being received.

- **Unacceptable use of the internet at St Margaret's Anfield CE Primary School**

Unacceptable use of the internet is not tolerated. Pupils, staff and governors should be aware that the following activities, whilst not an exhaustive list, are unacceptable:

1. The access to or creation, transmission or publication of any offensive, obscene or indecent images, sound, data or other material.
2. The access to or creation, transmission or publication of any data being displayed or converted to such obscene or indecent images, sounds data or other material.
3. The creation, transmission or publication of any material which can cause offence, inconvenience or needless anxiety.
4. The creation, transmission or publication of any defamatory material.
5. The receipt or transmission of material such that the material infringes the copyright of another person or infringes the conditions of the Data Protection Act 1984.
6. Activity that threatens the integrity of school ICT systems, or activity that attacks or corrupts other systems.
7. Use for personal financial gain, gambling, political purpose or advertising is forbidden.
8. Posting anonymous messages and forwarding chain letters is forbidden.
9. The transmission of unsolicited commercial or advertising material to other Net users.
10. The deliberate unauthorized access to facilities, services, data or resources via the internet.
11. Activities such as:
    - wasting staff or other users' efforts or network resources,
    - accessing or destroying other users' data.
    - violating the privacy of other users.
    - disrupting the work of other users.
    - using the internet in a way that denies service to other users.

Sanctions

If any breach of conditions is discovered, the incident and any outcomes will be recorded and the following sanctions may be enforced:

- Temporary or permanent ban on internet use.
- Additional disciplinary action in line with school behaviour policies.
- Parents and other external agencies may be contacted.

Summary

The safeguards St. Margaret's Anfield CE Primary School has put in place to protect children and staff are:

- communicating the conditions and expectations of use to all users.
- providing all children a copy of the rules for using the internet.
- providing a list of unacceptable uses of the internet.
- use of software to filter out unacceptable material.
- teachers ensure that children know how to use the internet safely and are taught e-safety explicitly in every year group every term.
- children understand the sanctions if any rules are broken.

Help:

- Children can call Childline free on 0800 1111 or access their website at www.childline.org.uk. You can talk to someone in private and it won't show up on your phone bill.
- www.thinkuknow.co.uk – a website for children, parents and teachers.
- CEOP – a website for children, parents and teachers to report abuse. www.ceop.police.uk/safety-centre

Other policies and documents which work alongside this policy include:

- Anti-bullying policy
- Safeguarding policy
- Behaviour Management Policy
- Security and data management policy
- Liverpool and DfE e-Safety guidelines.

Wider Reading

Diocese of Liverpool "Protecting yourself when using social media – A guide for schools and school leaders".

ADDITIONAL INFORMATION FOR STAFF

Internet Access
Internet access on school equipment (laptops/Macbooks/ipads) is restricted to the school site, the staff's own home or other locations authorized by the SLT. Home usage of the internet is a personal choice.

Permission must be sought from the Headteacher before downloading any programs onto school equipment.

Passwords
All staff must ensure that their laptop is password protected. The password should not be easy to guess e.g. it cannot be 'password' or 'margarets' or 'anfield'.

They must not share the password with anyone without the approval of the Headteacher.

If laptops are used by anyone other than the named keeper, the keeper must **directly and closely supervise** their use. You are fully responsible for your laptop/Macbooks.

Data Protection
You have a duty to take sufficient measures to ensure that the files stored on your laptop/Macbooks e.g. assessment records, school reports, photographs of children are securely protected. **This is why passwords are necessary** and also why no-one else should use your laptop/Macbooks unless under **close and direct** supervision.

Shopping
Browsing or shopping on retail websites for school resources using school equipment must be authorized by the SLT.

Barred List
This list is not exhaustive and your own professional judgment about what type of sites should be accessed is necessary. **If you think there may be a risk involved then do not take it.**

The following sites **must not be accessed** by staff on the school network or on school laptops/Macbooks:

- **shareware' sites which download (and upload) music/videos illegally**
- **Social networking sites for over 13s e.g. 'MySpace' 'facebook' and 'MSN' 'Twitter' 'Flickr' 'YouTube'**
- **Sites with potentially adult content (profanity/pornography) such as 'YouTube'**

Personal Photos
If personal photographs are stored on school equipment you should make sure they are not personally compromising. School will not take any responsibility for the loss of these items.

Mobile Phones
Staff must not use their mobile phones when responsible for supervision of children i.e. on the yard, in class, in the ICT suites, in the hall during lunchtime. Use for photographing pupils must be authorized by SLT.

Additional Advice
Internet use on your own equipment is obviously your own choice but as adults who work with children we all need to be safe.

If you choose to use social networking sites at home, you are advised to set the security and privacy settings so that no-one can view your page without your permission.

Never give out your personal email address or mobile phone number to children or parents.

Many teachers have had problems with social networking sites such as 'Facebook' 'MySpace' and 'Twitter' because children have accessed their page or the teacher's friends' pages to see the teacher concerned drunk or in their bikini or both! It is totally unacceptable to be 'friends' with SMA children, ex SMA children under 18 or any child who is posing to be older then they are on social networking sites, e.g. facebook is for children 13 or older, a child who is under 13 has lied about their age to access this site.

Teacher Unions
The main teaching and support staff unions have produced common-sense guidelines for teachers which are well worth reading.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- 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 child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy).
- Pupils and parents will be informed of consequences for pupils misusing the internet.

Reviewed by SLT 09.01.2014.