St Margaret's CE Primary

E-Safety Policy - Staff – 2012

This policy has been created using Lincolnshire' Safeguarding Children's Board and in conjunction with the Acceptable Usage Policy. E-Safety is an integral part of safeguarding at St Margaret's.

Policy Statement

Safety is a priority for the children and staff at St Margaret's. This policy includes guidance for children and adults on the safe use of Internet facilities in and outside of school. Technology is developing at an increasing rate and is now very much part of our everyday lives. Digital technology has many positive benefits, but we should be aware of the dangers we can be exposed to. It is increasingly common for schools to use technologies such as iPads, iPods and Nintendo Wii, which allow digital interaction. It is important that staff and children develop and apply appropriate skills in order to use technology safely both in and out of school. E-safety is the responsibility of all staff in the school. Parents will receive regular updates on safety through newsletters, the school website and parent evenings. We hope that this policy will ensure all adults in school can promote safety so that our children know how to use ICT safely at home too.

Internet access – You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues.

It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should you or a student of these sites unintentionally access you should report the matter to a member of the Senior Leadership Team so that it can be logged. Access to any of the following should be reported to Lincolnshire Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

Social networking – is blocked in our school, but safe use of recommended social networking sites, such as Club Penguin, are promoted where appropriate. This ensures children are aware of safe social networking sites which are available for young people, which require the consent of a parent or carer. Our Key Stage 2 e-safety policy provides a list of recommendations for keeping safe on social networking sites, in case our children are able to access these at home. Children at St Margaret's need to develop transferable skills, such as critical awareness, to apply both in school and at home.

Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that their profiles are not publicly available. Members of staff should never knowingly become “friends” with students or former students on any social networking site or engage with pupils on internet chat. Staff cannot mention anything at all to do with school life on social networking sites.

Use of Email - All members of staff should use their professional email address for conducting school business. Use of school email for personal/social use is at the discretion of the Head teacher.

Passwords - Staff should keep passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection - Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted, does it have to be on a USB memory stick which can be easily misplaced. All staff should be aware of the importance of keeping USB memory sticks safe and secure.

Mobile Phones – We allow staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a parent/carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate text messages between any member of the school community is not allowed. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Images and Videos - Staff and pupils should not upload onto any internet site images or videos of themselves or other staff or pupils without consent.

Use of Personal ICT - use of personal ICT equipment is at the discretion of the school. Any such use should be stringently checked for up to date anti-virus and malware checkers.

Viruses and other malware - any virus outbreaks are to be reported to Qegs as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Staff should note that internet and email may be subject to monitoring