St Bartholomew's CE Primary School

E-Safety Policy - Pupils

This policy has been created with a school emphasis using the e-safety policy of Lincolnshire Safeguarding Children's Board (LSCB) and the Acceptable Use of ICT Policy (AUP). This is a minimum requirement to which all school staff should adhere.

Responsibility – for e-safety in the school lies with the Head teacher and governing body but as with every other aspect of child safe guarding, every member of staff should be alert to any risks of harm that may arise through the use of technology in school.

Training – staff training will be provided annually by LSCB.

Teaching – Age appropriate E-Safety lessons are included within PSHE lessons as well as whenever using ICT across the curriculum wherein E safety could be an issue. E Safety awareness sessions are also provided for parents. Reference to the e-safety Dos and Don'ts poster should be made by members of staff whenever pupils are using the internet.

Policy

The use of ICT within St Bartholomew's has enormous benefits to education, however there are reasons why the school and the local authority must put some restrictions in place, such as: ICT equipment is very expensive to buy and maintain; the school and the local authority have a duty of care to ensure that you are safe and that you are not exposed to illegal or inappropriate content. It is hoped that these restrictions do not interfere with your education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues.

Please note that internet and email use may be subject to monitoring.

Use of the Internet - the internet is provided to help you with learning activities such as research, online activities, online educational games and many other things. The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. If you are unsure, or if you come across anything you feel is inappropriate, you should turn your computer monitor off and let your teacher know.

Logins and Passwords - every person has a different computer login. You should never allow anyone else to use your details.

Social Networking – We do not allow access to social networking sites (for example Bebo, Facebook, Flickr). Parents should check the access that children have to social networking sites at home, especially giving consideration to the age restrictions that apply to many sites.

If you do use sites at home remember you must not put photos or information about others on line without their permission. Also, it is not advisable to upload pictures or videos of yourself. Videos and pictures can easily be manipulated and used against you. You should never make negative remarks about the school or anyone within the school. Always keep your personal information private to invited friends only and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.

Some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognise. You should never meet a stranger after meeting them online. Always inform your parents about anybody you have chatted to on-line.

Security - you should never try to bypass any of the security in place. This security is in place to protect you from illegal sites, and to stop others from hacking into other people's accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that it is owned by somebody else and it is illegal to use this information without permission from the owner. If you are unsure, ask your teacher.

Etiquette – You have an email account at school. When you are sending a message always be polite and don't swear. Consider what you are saying, and how it might be read by somebody else. Without emoticons it is difficult to show emotions in things like emails and blogs, and some things you write may be read incorrectly.

Mobile Phones – We do not allow pupils to have mobile phones in school however those children that require them for after school use can store them in the school office.

Remember to always keep yourself safe when using your phone at home in the same way as when you are using the internet at home. Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else. In some circumstances this can be an illegal act.

Useful websites:
CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. There is an excellent educational programme, as well as advice and videos for all ages on their website.
www.ceop.gov.uk

IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content.
www.iwf.org.uk

Cybermentors is all about young people helping and supporting people online.
www.cybermentors.org.uk

Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same.
www.digizen.org

Reviewed and update: November 2014
Reviewed: June 2016
Reviewed: May 2017
Reviewed May 2018
Reviewed: November 2019
Reviewed: January 2021
Review Date: January 2022

Signed: ……Headteacher

Appendix 1

E-Safety Policy (do's and don'ts)

Some simple do's and don'ts for everybody (courtesy of CEOP):
Never give out personal details to online friends that you don't know offline.

Understand what information is personal: i.e. email address, mobile number, school name, sports club, meeting up arrangements, pictures or videos of yourself, friends or family. Small pieces of information can easily be pieced together to form a comprehensive insight into your personal life and daily activities.

Think carefully about the information and pictures you post on your profiles. Once published online, anyone can change or share these images.

It can be easy to forget that the internet is not a private space, and as result sometimes people engage in risky behaviour online. Don't post any pictures, videos or information on your profiles, or in chat rooms, that you would not want a parent or carer to see.

If you receive spam or junk email and texts, never believe the content, reply to them or use them.

Don't open files that are from people you don't know. You won't know what they contain—it could be a virus, or worse - an inappropriate image or film.

Understand that some people lie online and that therefore it's better to keep online mates online. Never meet up with any strangers without an adult that you trust.

Don't forget, it is never too late to tell someone if something or someone makes you feel uncomfortable.