THE EDWARD RICHARDSON PRIMARY SCHOOL TETFORD

E-SAFETY POLICY (PUPILS)

Review, Responsibility & General Information

Policy Category	Health & Safety
Review Cycle	Biennial
Body determining Review Cycle	Governing Body
Date of Governors meeting when last agreed	15th November 2016
Date of last review	7th November 2016
Term next due for update	Autumn Term 2018
Date due for next agreement by Governors	Spring Term 2019
Member of staff responsible for this update	Headteacher
Member of staff to whom queries are directed	Headteacher
Governor responsible for this update	Kevin Hyde
Requirement	Statutory

This policy has been created with a school emphasis using the e-safety policy of Lincolnshire Safeguarding Children's Board and the Acceptable Use of ICT Policy (AUP). We ask all parents to note the contents of the policy and discuss them with their children. The policy will also highlight some excellent tips relating to E-Safety at home!

E-Safety is short for 'Electronic' Safety. It is to do with staying safe when you are using equipment like ICT (computers and tablet devices – and especially the internet) and mobile phones.

The use of ICT within schools 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 intended that these restrictions do not interfere with the delivery of education, but if you feel otherwise you are encouraged to talk to a member of staff to discuss any issues. This policy is about how you use ICT at school but be aware that the same

dangers exist at home and it is always a good idea to talk to your parents or another sensible adult about these.

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.

Never try to bypass the security by using proxy sites, these are all monitored.

Logins and Passwords - every person has a different computer login and password. You should never allow anyone else to use your details. If you think someone else may have your details you should ask to have your password changed.

User Areas - your user area is provided for you to save school work. It is not to be used to save music or other files that you have brought in from home.

Social Networking - social networking (for example Bebo, Facebook, Whatsapp) is not allowed in your school. If you use such sites beyond school be aware of the age restrictions – they are there for a reason! You should never upload pictures or videos of others without their permission. 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. When you are old enough, and mature enough, to do so consider using a nickname and only 'inviting' people you know. Never create a false profile as a 'joke' or 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. It is recommended that you never meet a stranger in 'real life' after meeting them online. If,

however, you feel the need to do this, always inform your parents / carers and take one of them with you.

Security - you should never try to bypass any of the security in place, this includes using proxy bypass sites. 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 - many schools provide students with email accounts, or let students post on things like blogs. Always be polite. 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 - Some modern mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. However, in the same way that some internet services can be used inappropriately, the same is true with mobile phones. Your school does not allow mobile phones. Never take inappropriate or 'silly' pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate or 'silly' pictures that you have received from somebody else. In some circumstances this can be an illegal act. Respect the age restrictions on sites.

Useful websites:
CEOP is a part of the UK police force dedicated to the eradication of child 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
BBC - a fantastic resource of e-safety information for the younger child.
www.bbc.co.uk/cbbc/help/web/staysafe
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

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 about things online and that therefore it's better to keep online friends 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.