E-SAFETY & CYBER BULLYING

Glossary Answers

AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection Centre
Cyber Bullying	Bullying using technology such as computers and mobile phones.
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
Frape	Facebook Rape

Glossary Answers

Grooming	'A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
Hacker	Originally thought of as a computer enthusiast, but now is normally used to refer to computer criminals, especially those who break into other people's computer networks.
Impact Level	These indicate the sensitivity of data and the associated protection . The scheme uses five markings, which in descending order of sensitivity are: TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. Most pupil or staff personal data that is used within educational institutions will come under the PROTECT classification, however some (for example the home address of a child (or vulnerable adult) at risk) will be marked as RESTRICT.

Glossary Answers

Lifestyle Website	An online site that covertly advocates particular behaviours and issues pertaining to young and often vulnerable children for example anorexia, self-harm or suicide.
Phishing	This is an attempt to trick people into visiting malicious websites by sending emails or other messages which pretend to come from banks or online shops; the e-mails have links in them which take people to fake sites set up to look like the real thing, where passwords and account details can be stolen.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.

Glossary Answers

SGII	Self-Generated Indecent Image
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).

The Byron Review and Recommendations

- Her report recognised the advantages of new technologies and the ease and confidence with which children and young people use them. At the same time, the report emphasised that children and young people do not always have the knowledge, skills and understanding to keep themselves safe.

Being safe and being responsible

- Children who hold a parent's hand every time they cross the road are safe. However, unless they are taught to cross the road by themselves, they might not learn to do this independently. A child whose use of the internet is closely monitored at school will not necessarily develop the level of understanding required to use new technologies responsibly in other contexts.

- The most successful e-safety in homes and school is where children understand the risks and behave responsibly but also are aware of what to do when something goes wrong. Its just like teaching them to ride a bike!

Hints and Tips for Home

Parental Controls – On Everything digital !

- TV
  Games Console (PS3, Xbox, PSP…)
- Mobile Phone
- Laptop

Time Limits, Age Ratings

-Go to ISP provider – block through IP address

-Use Anti-virus software

Beware of system weaknesses!

don’t BE NAÏVE – real world situation

Difficult conversations with others

Hints and Tips for Home

- Safe Mode
- YouTube settings
- Google Search
- THINK before SHARE – would I SHOW IT IN ASSEMBLY?
- Facebook – Age restrictions! (13 minimum!)
- REPORT ISSUES

Safe Surfing

Extended Validation (EV) SSL Certificates (such as GlobalSign ExtendedSSL):

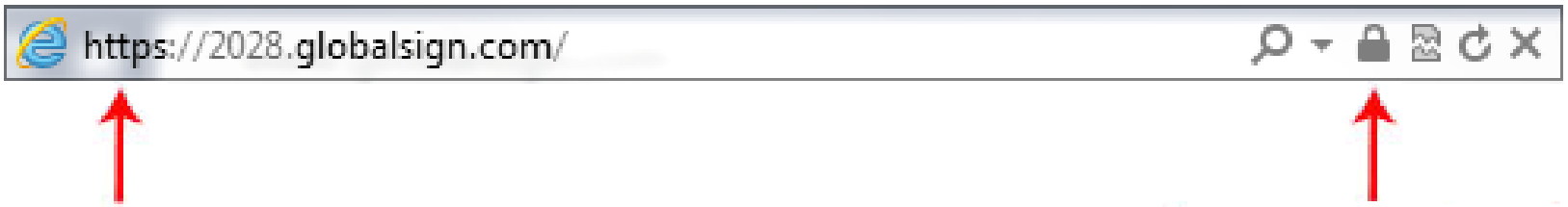
The address bar turns from white to green, indicating to visitors the web site is using Extended Validation SSL.

The web site owner's legally incorporated company name is displayed prominently on the address bar real estate. Extended Validation SSL is the only way for a company to get it's name displayed in the browser address bar.

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

Standard SSL Certificates (such as GlobalSign DomainSSL and OrganizationSSL) display:



The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL.

The padlock is activated, showing you that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, the page does not use SSL.

- [ ] Talk to your child about online grooming - Visit www.thinkuknow.co.uk
- [ ] Talk to your child about their online friends
- [ ] Let your child know that you understand and are always there for support
- [ ] Learn how to report any inappropriate contact made to your child online - Visit www.ceop.police.uk

6-9 Year Old Checklist

CREATE a user account for your child on the family computer with appropriate settings and make the most of Parental Controls and tools like Google SafeSearch

AGREE a list of websites they're allowed to visit and the kind of personal information they shouldn't reveal about themselves online (like the name of their school or their home address)

DECIDE time limits for things like using the internet and playing on games consoles

BEAR in mind what older siblings might be showing them on the internet, mobiles, games consoles and other devices and agree some rules as a whole family

TALK to other parents about their views on things like what age to buy kids a mobile and don't be pressured by your child into letting them use certain technologies if you don't think they're old enough or mature enough... no matter how much they pester you

FAMILIARISE yourself with age ratings and descriptions on games, online TV, films and apps, so that you can be sure your child is only accessing age-appropriate content

10-12 Year Old Checklist

MAKE sure you've set some tech boundaries before they get their first mobile or games console – once they have it in their hands, it can be more difficult to change the way they use it

REMIND your child to keep phones and other devices well hidden when they're out and about to minimise the risk of theft

TALK to them about what they post and share online – written comments, photos and videos all form part of their 'digital footprint' and could be seen by anyone and available on the Web forever

DISCUSS the kind of things they see online – this is the age when they might be looking for information about their changing bodies and exploring relationships, for example

HOLD the line on letting your son or daughter sign up for services like Facebook and YouTube that have a minimum age limit of 13 – talk to other parents and their school to make sure everyone is on the same page

REMIND them that they shouldn't do anything online that they wouldn't do face-to-face

What students are expected to know

- If you felt uncomfortable about anything you saw, or if anybody asked you for your personal details such as your address on the internet would you know where to go for help?
- If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
- Can you tell me one or more of the rules your school has for using the internet?
- Can you describe the risks of posting inappropriate content on the internet?

Areas of Risk to be aware of

content: being exposed to illegal, inappropriate or harmful material

contact: being subjected to harmful online interaction with other users

conduct: personal online behaviour that increases the likelihood of, or causes, harm.

- **Content**
- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

- **Contact**
- grooming
- cyber-bullying in all forms
- identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

- **Conduct**
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Cyber Bullying

1st Peak 10 -11 (first get online chat /text / email/gaming)

22% of 8-11's have ….

2nd Peak 14 -15

12-15' have …….

Is it a girl thing?

Reporting rate is higher.

In 12-15 age group girls send more than 30 texts per day – 35% more than boys. (OFCOM 2012)

Idea of a friend

Is it OK to?

- Girls reporting rate is higher!
- Gender specific routes to bullying