Glebe School

E-Safety

Last Updated Sept 2021

Initial Report into E-Safety

Contents

E-Safety Mission Statement

Glebe School is committed to raising standards in e-safety with an objective to;

- **Protect** and **educate Pupils** and staff in their use of technology

- To have the **appropriate mechanisms** to intervene and support any incident where appropriate.

The main threats identified in terms of e-safety are as follows;

- **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.

Report Objective

This report will look to identify current procedures undertaken in regards to e-safety within the school. It will identify areas that need to be improved in order to meet the outstanding Ofsted framework for e-safety at Glebe School.

Overview of Whole school approach to e-safety

In the five schools judged outstanding by Ofsted for e-safety, all staff members had a shared responsibility for installing e-safety within the school. In order to catalyse this at Glebe school, I recommend the implementation of the following steps.

- 3 engaging assemblies per year (1 per term) to raise awareness in regards to different e-safety related issues. One of these should be held on "Safer internet day" to raise awareness (11 February 2014).

- Cross curricular links to incorporating e-safety into the curriculum (See Below), this could also be part of an "e-safety awareness week".

  – English: story writing exercise to develop a character who has been effected by a chosen e-safety risk.
  – Drama: Role play exercises which enable students to act in character in relation to e-safety related issues.
  – ICT: E-safety Leaflet design project (Already Implemented)
  – Maths: Looking at data in relation to e-safety and plotting it into graphs / pie charts.
  – PSHE: Poster design project where students look at e-safety risks and raise awareness in the local community using their poster design.

Outstanding schools also had excellent relationships with families, which needs to be developed further in order to continue e-safety support at home. In order to meet this criteria at Glebe I recommend the following steps;

- Hold a student / parent audit, gaining information on how students and parents currently feel about e-safety and how they would deal with certain e-safety related issues, should they arise. This information can

aid the development of e-safety within the school and meet the needs of the pupils.

- Add a tab to the website that enables parents to receive up-to-date information in regards to e-safety and different resources to raise awareness. This would be advertised to the students and the parents.

Staff Training

The weakest aspect of provision in the schools visited was the extent and quality of training for staff. It did not always involve all staff, and even when it did, its impact what not measured systematically. I recommend we undertake the following steps in order to tackle these issues.

- Audit the training needs of staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies.

- Use audit results (of both staff, parents and students) to develop e-safety strategies.

- Review and develop e-safety procedures to ensure they have a positive effect on pupils' knowledge and understanding.

Specialised risks to students at Glebe

Students with SEN are 16% more likely to be victims of online abuse; children from lower socio-economic groups are 12% more likely. Issues are magnified for 'vulnerable' children (e.g. disabled students, pupils with SEN or looked after pupils).

Short term goals for e-safety within the school

- Passwords must be given to each pupil to ensure their effective use. Their e-mail passwords could be used to avoid confusion. Although this may pose initial problems with students forgetting passwords, it is an important step that needs to be taken to fall in-line with Ofsted criteria.

- School-based reporting routes should be clearly understood and used by the whole school. A good way to do this would be to utilise an online anonymous reporting system. When and if this is set up, pupils and parents should be made aware of this via assemblies and newsletters.

Long term goals for e-safety within the school

- It is advised that e-safety should be a priority across the whole school and achieving the **e-safety mark** would be a good long term objective to accredit the schools progress with e-safety within the school.

- All teaching and non-teaching staff should receive regular and up-to-date training. In order for myself to have an added insight into e-safety, it may be beneficial to attend a course in order to pass on expertise to the staff at Glebe. This is important to meet the outstanding criteria of "One or more members of staff have a higher level of expertise and clearly defined responsibilities."

- Rigorous e-safety guidelines and procedures to be in place which are contributed by the whole school. These should be updated regularly and

ratified by the school governors. This policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying.

- To develop risk assessments in relation to e-safety, using data to assess the impact of e-safety practice and how this informs strategy.

- Parent's e-safety twilight sessions to raise awareness.

- Development of an e-safety handbook / poster to send out to parents for advice.

Example of questions that could be asked in an audit for students:

1. 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?
2. If anybody sent you hurtful messages on the internet or on your mobile phone would you know who to tell?
3. Can you tell me one of the rules your school has for using the internet?
4. Can you describe the risks of posting inappropriate content on the internet?

Sample questions for staff:

1. Have you had any training that shows the risks to your and pupils online safety?
2. Are there policies in place that clearly demonstrate good and safe internet practice for staff and students?
3. Are there sanctions in place to enforce the above policies?
4. Do all staff understand what is meant by the term cyber-bullying and the effect it can have on themselves and pupils?
5. Are there clear reporting mechanisms with a set of actions in place for staff or pupils who feel they are being bullied online?
6. Does the school have any plans for an event on safer internet day?

In a good school Ofsted expect positive answers to the above questions. This demonstrates the staff's awareness training outlining what the current risks are and what resources are available to help them keep pupils and themselves safe online.

Glossary

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use http://www.digizen.org/glossary/. In addition, the following terms used in this document are explained below

|	
Age related filtering	and dependent on age and appropriate need (commonly used providers include Smoothwall, Lightspeed, Netsweeper, RM).
AUP	Acceptable Use Policy
Byron Review	Professor Tanya Byron's seminal report from 2008, 'Safer Children in a Digital World' available at http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.
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.
EPICT	European Pedagogical ICT Accreditation.
E-safety mark	Accreditation for schools reaching threshold levels within 360 degree safe through assessment by external assessor.
Frape	Short for 'Facebook rape', referring to when a Facebook user's identity and profile are compromised and used by a third party to cause upset.
Games Console	Examples include XBOX 360, Nintendo Wii, PlayStation 3, and Nintendo DS.
Grooming	Online grooming is defined by the UK Home Office as: '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 a hacker is normally used to refer to computer criminals, especially those who break into other people's computer networks.
Impact level	Impact levels indicate the sensitivity of data and the associated protection required (see the government published HMG Security Policy Framework http://www.cabinetoffice.gov.uk/spf). 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.
ISP	Internet Service Provider (a company that connects computers to the internet for a fee).
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.
Locked down system	In a locked down system almost every website has to be unbarred before a pupil can use it. This keeps the pupils safe, because they can use only websites vetted by their teachers, the technicians or by the local authority, any other website has to be unbarred for a pupil to be able to use it, which takes up time, detracts from learning and does not encourage the pupils to take responsibility for their actions (note that a locked down system may be appropriate in an EYFS setting or in a special school).
Malware	Bad software or programs that damage your computer (viruses), steal your personal information (spyware), display unwanted adverts (adware) or expose your computer to hackers (Trojan horses).
Managed system	In a managed system the school has some control over access to websites and ideally offers age-appropriate filtering. Pupils in schools that have managed systems have better knowledge and understanding of how to stay safe than those in schools with locked down systems because they are given opportunities to learn how to assess and manage risk for themselves.
Phishing	Pronounced the same as 'fishing' 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.
Profile	Personal information held by the user on a social networking site.
RBC	Regional Broadband Consortium, often providers of schools broadband internet connectivity and services in England, for example SWGfL, London Grid for Learning (LGfL).
Safer Internet Day	Initiated by the European Commission and on the second day, of the second week of the second month each year.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
SGII	Self generated indecent images (often referred to as "sexting" – see above)
SHARP	Example of an anonymous online reporting mechanism (Self Help And Reporting Process).
SNS	Social networking; not the same as computer networking, social networking is a way of using the internet and the web to find and make friends and stay in touch with people.

E-safety progress report – 4th march 2014

Safer Internet Day

To recognise safer internet day as a school, we had a number of events and activities taking place to raise awareness and participation.
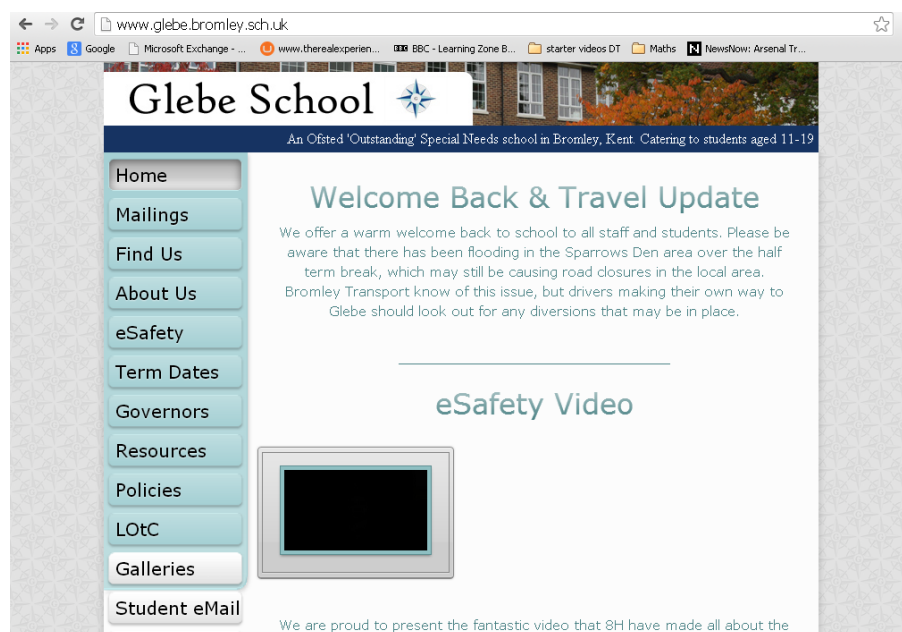
E-safety video

Students in year 8 created a fantastic e-safety video which is available to view on the website. Students outlined a number of dangers online and explained to fellow students, the process to follow if problems occur online. This video was shown during the assembly during safer internet week.

Assembly

Students were shown the year 8 e-safety video during assembly, which took place during safer internet day. Students were engaged during the assembly and also gained important information about e-safety. This adds to the schools objective to have a whole school approach to e-safety in schools.
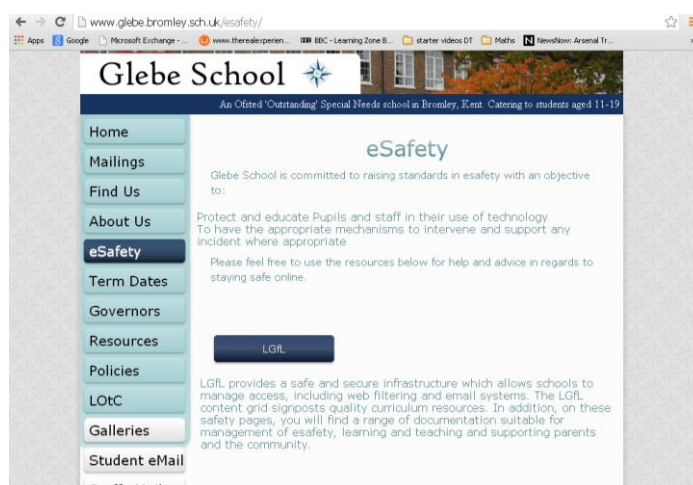

Network Desktop Background

During safer internet week, we changed the background for all the computers connected to the schools network. This further raised awareness to students in regards to being safer online.

E-Safety Tab on website

We have added a tab on the website for students and parents to get up-to date information in regards to e-safety. The page has useful links to LGfL and Think You Know. This page will continue to be updated and developed, alongside the new website that is being created for the school.

Risk Assessment

We are looking to implement a risk assessment in order to deal with any e-safety issues as and when they arise. This will also help prevent e-safety risks occurring through policies and procedures.

Risk Log
(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3		e-Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	e-Safety Officer IT Support
2.	Blogging	Inappropriate comments	2	1	2	e-Safety Officer IT Support
2.	Blogging	Using copyright material	2	2	4	e-Safety Officer IT Support
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	e-Safety Officer IT Support

Likelihood: How likely is it that the risk could happen (foreseeability).
Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.
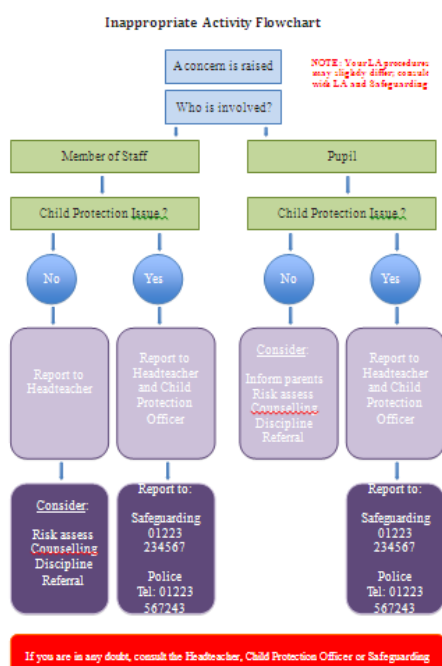Final decision rests with Headteacher and Governing Bod

12

Incident Log

We are considering implementing an incident log to document any issues that arise in relation to e-safety. This will help us analyse incidents and their level of severity in order to best prevent them from re-occurring. This will be held in a red folder in both ICT rooms.

e-Safety Incident Log

Number:	Reported By: *(name of staff member)*	Reported To: *(e.g. Head, e-Safety Officer)*
	When:	When:
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)		
Review Date:		
Result of Review:		

Flow Chart

We have developed a flow chart for illegal activity and inappropriate activity. This will best enable staff to be aware of procedures and also what to do when an issue arises. This will be kept in the e-safety folder in both ICT rooms.

Inappropriate Activity Flowchart

A concern is raised

NOTE: Your LA procedures may slightly differ, consult with LA and Safeguarding

Who is involved?

Member of Staff → Child Protection Issue? → No → Report to Headteacher → Consider: Risk assess Counselling Discipline Referral

Member of Staff → Child Protection Issue? → Yes → Report to Headteacher and Child Protection Officer → Report to: Safeguarding 01223 234567 Police Tel: 01223 567243

Pupil → Child Protection Issue? → No → Consider: Inform parents Risk assess Counselling Discipline Referral

Pupil → Child Protection Issue? → Yes → Report to Headteacher and Child Protection Officer → Report to: Safeguarding 01223 234567 Police Tel: 01223 567243

If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding

Letter to parents

13

We have devised a letter to be sent out to parents in the Easter newsletter. This could also be included in the planner and in the induction pack to new students coming to Glebe. This will raise awareness for parents and students alike.

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access sites such as this. We are able to do this using advanced software known as an Internet filter.

The software also allows us to block potentially dangerous websites, whilst still ensuring your child can use the internet as a positive educational resource. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

You may also have noticed that we have added an e-safety link on our website. This section of our website provides useful links and resources to keep you up to date on keeping your child safe online.

If you have any questions or concerns please contact admin@glebe.bromley.sch.uk.

Yours Sincerely

_____

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian –

Name of Child –

Signature -   Date

E-Safety Meeting Minutes

Date: 23/10/14
Time:12:00pm

Topics:

1. **E-Safety Mark** - It has been agreed that WH will look into E-Safety mark to investigate qualifying criteria to then discuss with DB/KS if it is a viable accreditation going forward.

2. **CEOP Reporting Link** - DB will look into inserting a CEOP reporting link on the E-safety tab on the website.

3. **Edublogs** - It has been agreed that WH will look into moderating privileges for teachers and level of control that the teacher has on publication of student blog posts. A decision as to whether to use the site in the ICT curriculum will then be made by WH/DB/KS based on those findings. An ICT blog which is controlled by WH only should be able to go on the website with KS permission, with all updates being approved by KS prior to publication (TBC).

4. **New E-safety video** - A new year 8 E-safety video will be created this year in ICT and published under the E-safety Tab on the website, different to last years. Confirmation of students who's faces are not allowed to be shown in video has been sought. This could be published for internet safety week which is on Tuesday 10th February 2015.

Meeting ended: 12:30pm.

Update: 03/07/15

E-safety Video

Year 8 students created an e-safety video in accordance with the annual e-safety leaflet project. We invited the students to come up with the scripts, ideas and themes of the video and the video can be seen under the e-safety tab on the website.

This continues to raise awareness with Students, staff and parents at glebe school on E-safety related issues.

Safer Internet Day 2015

Glebe celebrated safer internet day. We held an assembly, where we showed students the e-safety tab on the website and also showed them the video that year 8's had made. We changed the backgrounds on all the network PC's which also raised awareness on a whole school basis.
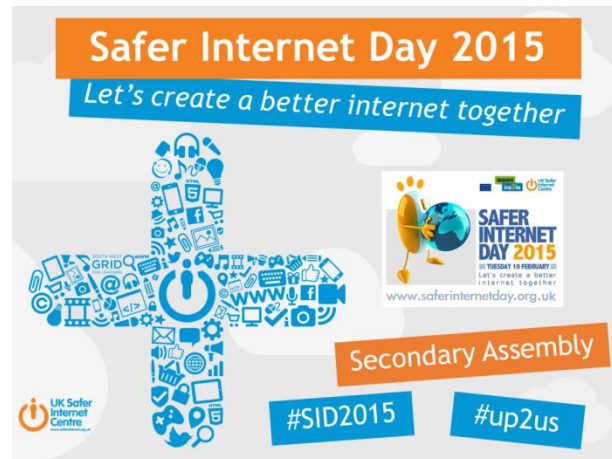
New Year 7 E-safety Comic Book Project

In an attempt to increase E-safety in the ICT currculum, we have introduced a new year 7 Comic book project. This project is focussed on students creating their own superheroes and combining these with an e-safety related narrative.

IAP Day Parents E-safety Workshop

In an attempt to raise awareness of E-safety related issues amongst our parents, we ran an E-safety workshop for parents on IAP day. The idea was to give parents some information on E-safety and point them in the direction of excellent esafety related resources and services online. We also wanted to raise awareness of the esafety Tab on the website, for all the latest information on E-safety related to Glebe. We produced some booklets to go alongside the even and also an annonymous questionnaire which is intended to give us more information about our parents and issues that they may need more advice on. This will be sent out with the summer newsletter, which will go to all parents, in order to hopefully get a better indication, from a broader range of parents. These resources will all be placed on the website to be utilised by the parents.
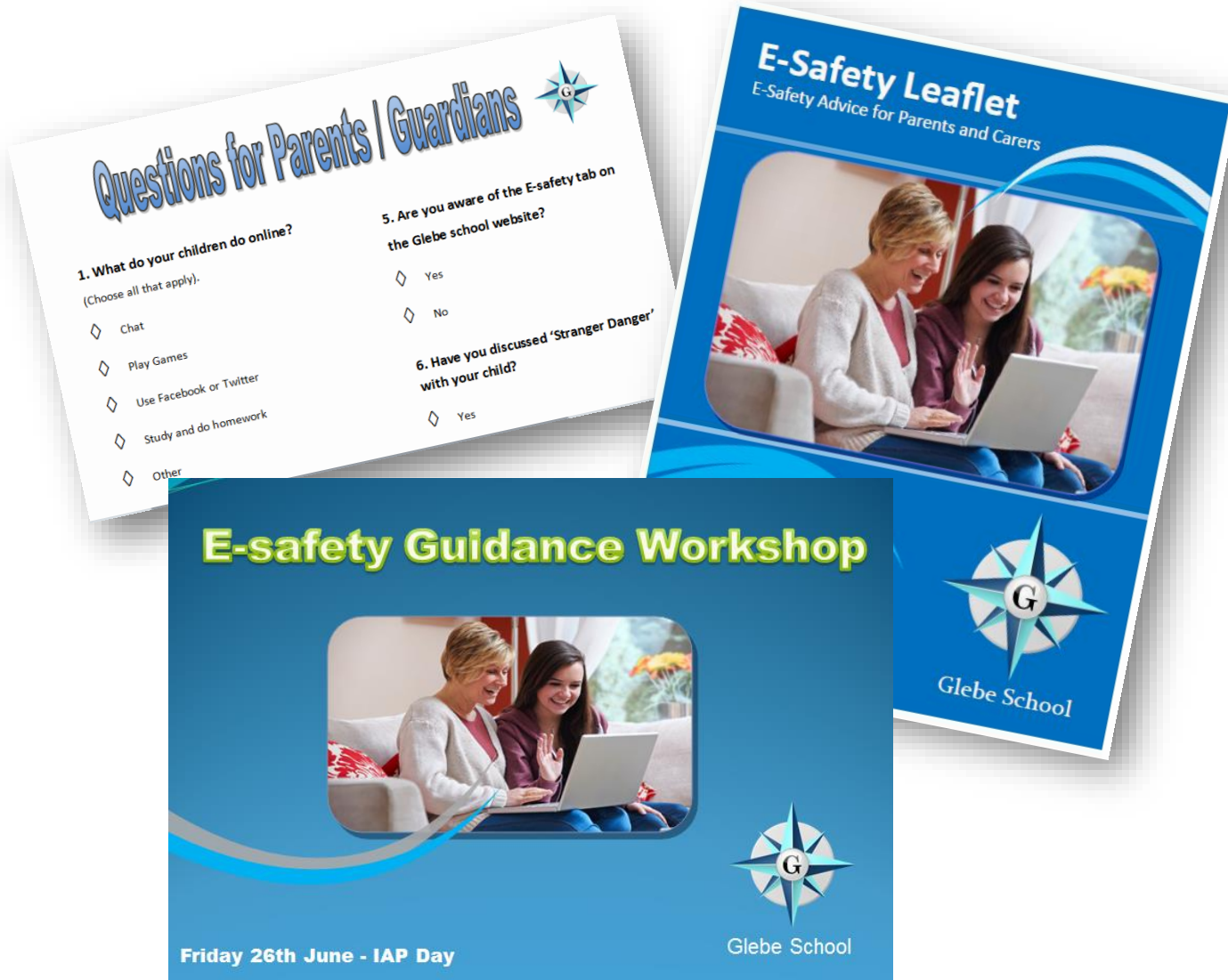
E-Safety video 2016

This years E-safety video is a great addition to previous years videos and further extends the knowledge of E-safety related issues in and out of the school context. Students this year produced a video themed on their favorite superheroes in an attempt to warn pupils about E-safety.

E-Safety Tab Update

The E-safety tab on the website is really starting to take shape now. We now have a RSS feed which gives parents the latest tips and advice on E-safety related issues directly from the governement. This ensures the tab is a great resource for parents, gives a range of links, resources and the ability to view past Esafety videos that the children have made. We have also added a CEOP reporting link that enables students to report incidents online with ease. We have told the students about this link and ensured that they are responsible when using it.
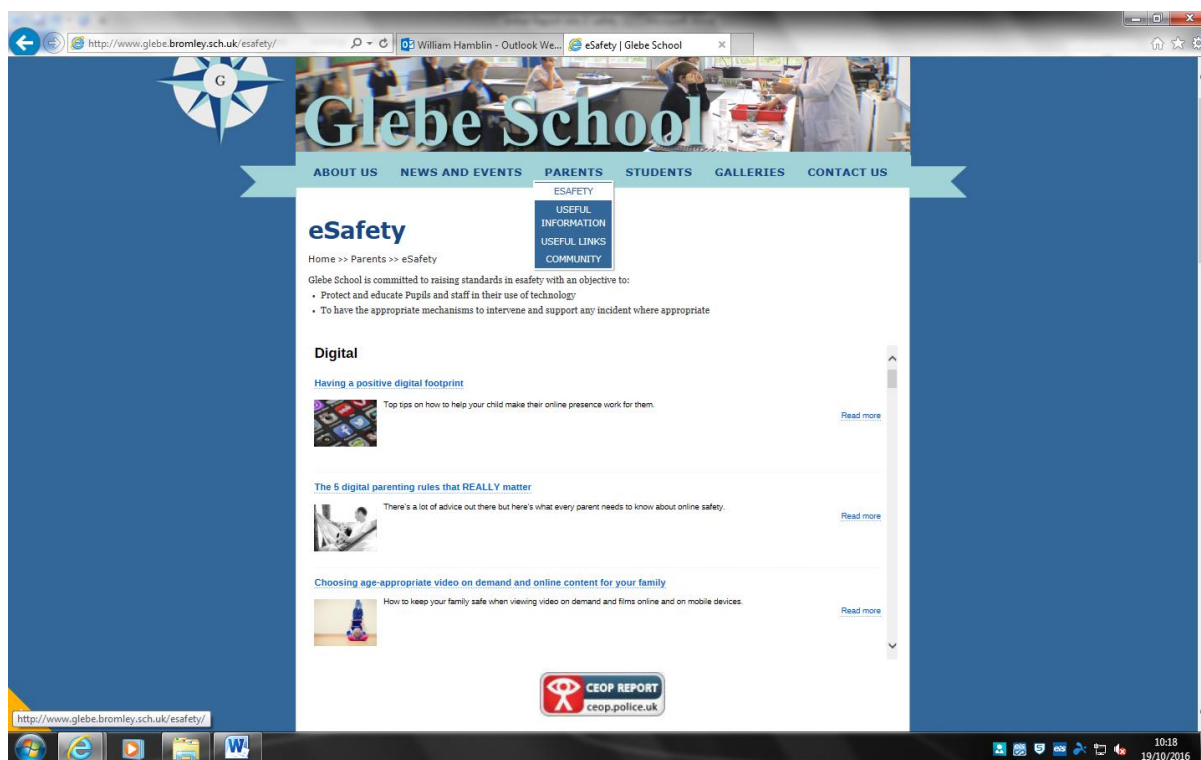
E-Safety Mark

We have been given the go ahead to try for the E-Safety Mark by KS. We have looked at the criteria set by the mark and we are pleased with how close we are to meeting the main strands. We have systematically gone through this and made notes on how we are meeting them, or what we need to do in order to do so.

 Areas of improvement are raising awareness amongst the whole staff with E-safety related issues. We also need to involve the children in the policy making for Esafety within the school, taking ownership of the sanctions and rewards put into place. We are going to ask the Student Council to generate these, which is something they have already started doing. Below is the PowerPoint designed to facilitate this.

We will also look to deliver the CEOP ambassador training to the whole staff. This has been scheduled to take place in March 2017. This is a certificated course and will ensure all staff members are fully equipped to deal with and E-safety related incident. It will also fulfil the last criteria needed for the E-safety Mark. This can also be opened up to other schools that we have an alliance with.

 'Sexting' in schools: advice and support around self-generated images What to do and how to handle it

We have distributed this advice leaflet to staff via email. A hardcopy is also available in the E-safety incident folder, which we felt was the most appropriate and accessible place for referral.

Breck Foundation Visit

We recently had a talk from the Breck Foundation, who spoke to years 8-13 students. The Breck Foundation is raising the awareness of playing safe whilst using the internet. Breck Bednar was a 14 year old boy, from Caterham, Surrey who loved technology and online gaming. He was groomed via the internet and murdered on February 17th 2014 by someone he met online. This foundation has been set up in his memory to help other young people enjoy playing online but crucially to be aware of some simple rules to stay safe. We arranged this to be in conjunction with the **Safer Internet Day 2017** and the talk had a great impact on all the students.

Safer internet day was celebrated in our usual way, of showing the students the E-Safety video that the year 8's created this year. The video went down really well and the students were engaged throughout. We also changed the background of every computer to emphasise this.

E-Safety Policy

As part of the feedback from the Challenge partners review, we have developed a more defined 'keeping children safe online policy'. Although a lot of our initiatives and protocols are listed in this document, it is better to have a concise document which has all our main procedures contained within it. This document has been approved by the governors and is now visible on our website.

CEOP Ambassador Training

All teaching staff have now received the CEOP ambassador training. It is excellent to have a whole school awareness of teaching staff on this whole issue and staff are now equipped to deliver the training to children. All safeguarding policies were revised during the presentation.

WRAP Prevent training

All staff recently completed the WRAP 'Prevent' training. The chair of governors was also present which demonstrates their ongoing involvement in E-safety related training. All staff have also completed the online based training, which makes us up to date with the most recent training on Prevent.

E-Safety video

Students in year 8 have been working really hard to produce the Glebe 2018 E-Safety Video. The video was directed and written by students in year 8 and they themed it on superheroes to raise engagement. The video will be uploaded to the website and will be shown in the whole school assembly.

Termly E-Safety Meeting

We have started having Termly E-safety meetings with representatives from students, teaching staff, parents and governors. This is aimed to discuss new updates for E-safety at Glebe and discuss targets for the future to make Glebe a safer online community. The minutes for these meetings will be placed online for all to see.

Impero

The school has invested in Impero software which uses key logging to flag keywords that may be of concern. The software takes a 15 second clip of what is happening on the screen, which adds context. We can also target students independently and educate them on appropriate usage of the internet based on the issue that was flagged. This has always proven to be successful in the early trial period. We are looking to develop a computer based E-safety log folder where staff can log an incident and explain what action was taken. This reduces the need to generating lots of physical paperwork and also means that logs can be stored digitally rather than needing to be printed every time there is an incident.

AUP Policy

We have included an AUP for student's every time they log in. This reminds students of our expectations of them when they use computers and the internet. The AUP is very simple to ensure students understanding of it.

Students also sign an AUP at the start of the year which is 'SEN' friendly. This is explained to them during Tutor time, so they understand what they're agreeing to.

Student Council – E-Safety Incident Sanctions

Students from the school council have been asked to generate some sanctions for different incidents that may occur relating to E-safety in the school. We wanted the students to play an active role in this. The rules will be agreed and moderated if necessary by SLT. They will then be shared with the whole school in assembly and / or literacy periods.

New E-Safety Incident log

We have developed a digital E-safety incident log to log e-safety related incident and their outcomes. It was decided that with the addition of Impero – which generates digital reports, we should have a digital means to store and document these instead of printing the reports and logging them in a physical folder. Incidents that are low level are passed on to the Form tutor to deal with pastorally. When an incident re-occurs or is of a more serious nature, the incident will be logged and dealt with by HoY or a member of SLT. This folder that we store the incidents is only accessible by MLT and SLT. Safeguarding protocols will be followed where appropriate and necessary.

Google Internet Legends

We have introduced the 'Google Internet Legends' program to Glebe and have introduced this as a whole school agenda in 2019/20 term. Due to COVID we

have not yet delivered this to our current year 7/8 students, but plan to do so this academic year.

Lockdown Booklet

We sent a helpful Esafety lockdown booklet to inform parents of the dangers online, especially during the lockdown periods.

We have also reinforced this in our Summer newsletter.

CPOMS

We now have an online logging system 'CPOMS' which greatly improves communication of Esafety incidents between staff members. This also enables us to track actions taken into incidents and track patterns in behavior.