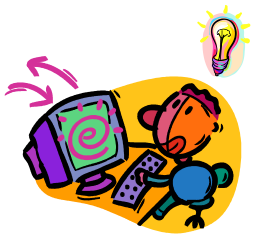
SAFEGUARDING CHILDREN ONLINE POLICY

Our Lady of the Visitation Catholic Primary School

Approved by:	Maureen Gordon	**Date:**	May 2016
Last reviewed on:	May 2018		
Next review due by:	May 2020		

Keeping Safe - Information & Communication Technology



E-safety – Acceptable Use Policy - Managing the Internet Safely

1. Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through, for example: communication systems; improved access to technical support, including remote management of networks and automatic system updates; online and real-time 'remote' training support; secure data exchange between local and government bodies.

In support of this, the government provides a Standards Fund grant to support Local Authorities procure broadband services through local Regional Broadband Consortia (RBC). In London the London Grid for Learning (LGfL) is the RBC. London schools are connected onto this broadband network. The LGfL is part of the National Education Network (NEN).

2. The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame' supportive culture if pupils are to report abuse. Risks can be high outside school, so the school will consider extending an education programme to parents and carers.

The School also needs to protect itself from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

The School will help protect itself by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised" and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff and for parents.

3. Technical and Infrastructure:

This school:

1. Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network
2. Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students
3. Has additional user-level filtering in-place using the Synetrix USO service
4. Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot run executable files such as .exe / .com / .vbs etc.
5. Ensures their network is 'healthy' by having Synetrix health checks annually on the network
6. Utilises caching as part of the network set-up
7. Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies
8. Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately
9. Never allows pupils access to Internet logs
10. Uses security time-outs on Internet access where practicable / useful
11. Uses individual log-ins for pupils from Y1 and all other users
12. Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful
13. Never allows personal level data off-site unless it is on an encrypted device (school provides encrypted USB memory sticks to staff)
14. Ensures pupils only publish within appropriately secure learning environments i.e. virtual learning environment / Fronter

4. Policy and Procedures:

This school:

1. Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access
2. Uses the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature
3. Has additional user-level filtering, to adapt filtering to the age of the pupils
4. Ensures staff previews all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform
5. Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required
6. Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search
7. Informs users that Internet use is monitored
8. Informs staff and pupils that that they must report any failure of the filtering systems directly to the school's ICT curriculum lead teacher; our systems administrators report to LA / LGfL where necessary
9. Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform
10. Only unblocks social networking sites for specific purposes e.g. Internet Literacy lessons
11. Only uses LGfL for pupil's own online creative areas such as web space and eportfolio

12. Only uses the LGfL / NEN service for video conferencing activity
13. Only uses approved or checked webcam sites
14. Has blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network
15. Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at the time of their daughter's / son's entry to the school
16. Requires pupils (and their parent/carer) from years 1 to 6 to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme
17. Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file
18. Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
19. Keeps a record e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour for learning system
20. Ensures the designated person for child protection has appropriate training
21. Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents
22. Immediately refers any material we suspect is illegal to the appropriate authorities – police and the LA

5. Expectations of Staff who work in the school:

Staff:

1. review and evaluate web sites prior to use with the pupils
2. whenever appropriate, use downloaded material rather than use the Internet 'live'
3. plan specific and focussed tasks for pupils using email or the Web
4. keep a check on the web pages pupils are accessing - this may also be done retrospectively by checking the History pages
5. monitor the email messages sent and received by pupils - in accordance with Department for Education guidance, pupils may often use communal email accounts
6. only use News Groups or Chat rooms after consultation with Ealing's ICT team.
7. report the Web address (URL) of any offensive material to either Edex / DIALnet or Ealing's ICT team
8. seek parent permission for use photographs of pupils on email attachments or web pages
9. construct web pages in such a way that the name of a pupil in a photograph cannot be deduced by an outsider viewing the web page. i.e. not have pupils' names alongside photos, nor use pupils' names in text which refers to a photograph

6. Education and training:

This school:

1. Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable
2. Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or curriculum lead teacher for ICT
3. Ensures pupils and staff know what to do if there is a cyber-bullying incident
4. Ensures all pupils know how to report abuse
5. Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance - pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion
- to develop a range of strategies to validate and verify information before accepting its accuracy
- to skim and scan information
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be
- to know some search engines / web sites that are more likely to bring effective result
- to know how to narrow down or refine a search
- to understand 'Netiquette' behaviour when using an online environment / email i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings
- to understand why they must not post pictures or videos of others without their permission
- for older pupils to understand why and how some people will 'groom' young people for sexual reasons
- to know not to download any files such as music files without permission
- to have strategies for dealing with receipt of inappropriate materials

1. Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights

2. Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate - this may include risks in pop-ups, buying on-line, on-line gaming & gambling

3. Ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities

4. Makes training available annually to staff on the e-safety education program

5. Runs a rolling programme of advice, guidance and training for parents, including:
   - information leaflets; in school newsletters; on the school web site
   - demonstrations, practical sessions held at school
   - distribution of 'think u know' for parents materials
   - suggestions for safe Internet use at home
   - provision of information about national support sites for parents.
   - lead awareness raising sessions for staff and parents on e-safety at least once every two years

Think before you click

S 

I will only use the Internet and email with an adult

A 

I will only click on icons and links when I know they are safe

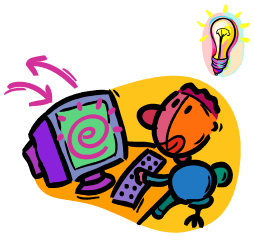
F 

I will only send friendly and polite messages

E 

If I see something I don't like on a screen, I will always tell an adult

Keeping Safe - Information & Communication Technology – key stage 2 agreement



RESPONSIBLE USE of COMPUTERS and the INTERNET

These 10 rules help us to be fair to others and keep everyone safe.

stop, think, before you click!

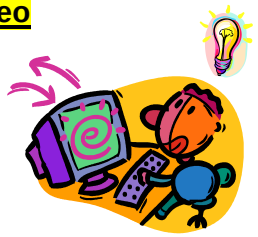
1. I will use only my own network login and password, which I will keep secret
2. I will only look at my own files and will not look at other people's files without their permission
3. I will ask permission from a member of staff before using the Internet
4. I will only e-mail people I know, or a person that my teacher has approved
5. I will always make sure the messages I send, or the information I upload, will always be polite and sensible
6. I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it
7. If I see anything I am unhappy with or I receive messages I do not like, I will not respond to it but I will immediately tell a teacher /responsible adult
8. I will ask for permission from my teacher if I want to bring software / files into school
9. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent / guardian / teacher has given me permission and I take a responsible adult with me

I understand that:

- the school may check my computer files and the Internet sites I visit
- if I deliberately break any of these rules, that I will not be allowed to use the computers / Internet in the school.

Keeping Safe - Information & Communication Technology

use of digital images - photography and video



To comply with the Data Protection Act 1998, we need parent / guardian permission before we can photograph or make recordings of the children. We follow these rules for any external use of digital images:

if the pupil is named, we avoid using their photograph

if their photograph is used, we avoid naming the pupil

Where showcasing examples of pupils work we only use their first names, rather than their full names. If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film. Staff are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used include:

- a child being photographed by the classroom teacher, teaching assistant or another child as part of a learning activity e.g. photographing children at 'work' and then sharing the pictures on the interactive whiteboard in the classroom allowing the children to see their work and make improvements

- a child's image is used for presentation purposes around the school e.g. in school wall displays and PowerPoint© presentations to capture images around the school or in the local area as part of a project or lesson

- a child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website. In rare events, a child's photograph could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or parents/guardian actually want a child's image linked to their name we would contact the child's parent/guardian for permission e.g. if a child won a national competition and wanted to be named in local or government literature.

Further information for parents on e-Safety can be found at:

http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

Our Lady of the Visitation Catholic Primary School

Keeping Safe - Information & Communication Technology

E-SAFETY INCIDENT REPORT LOG

Incident(s) reported by / when / to	
Name of Instigator (if known) **Date of Birth**	**Name of Victim** **Date of Birth**
Names of any witnesses	
Incident(s) took place: in school ( ) where: **at home ( ) elsewhere ( ) where:**	
Date(s) of incident(s)	
Description of incident(s) NB attach any evidence to this form	
Instigator: resulting action / follow up (if required) – who / when / what	**Victim: resulting action / follow up (if required) – who / when / what**
Parents informed? **when / by whom / how / parents response**	**Parents informed?** **when / by whom / how / parents response**
Log completed by:	**Date:**