Chorley St Mary's Catholic Primary School

E-Safety Policy

Reviewed May 2015
Next Review May 2016

Content

Introduction

The St Mary's E-Safety Policy has been produced from a template produced by the respected SWGfL Committee and is linked with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group / committee made up of:

- *Headteacher – Designated Senior Person for Child Protection and School E-Safety Officer*
- *Teachers*
- *Teaching Assistants*
- *ICT Technical staff*
- *Governors*
- *Parents and Carers*
- *Pupils*

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	*To be approved at standards and effectiveness committee 07/10/15*
The implementation of this e-safety policy will be monitored by the:	*Senior Leadership Team/ Computing Subject Leader*
Monitoring will take place at regular intervals:	*Once a year / May*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Autumn term standards and effectiveness committee*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*September*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *monitoring logs of internet activity via LGFL*
- *Internal monitoring data for network activity if possible*

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Standards and Effectiveness Committee of the Governing Body* receiving regular information about e-safety incidents and monitoring reports.

Head teacher and Senior Leaders:

- **The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *ICT Co-ordinator.*
- *The Head teacher is responsible for ensuring that the ICT Co-ordinator and E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant*
- *The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive monitoring reports from the E-Safety Co-ordinator / Officer.*
- **The Head teacher and the Deputy Head teacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

E-Safety Coordinator / Officer:

- has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- liaises with ICT Co-ordinator and the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

  The investigation / action / sanctions regarding incidents will be the responsibility of the E-Safety Co-ordinator or the Deputy Head Teacher.

Computing Co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Examples of suitable log sheets may be found in the SWGfL Safety and Security Booklet, along with the Internet Safety Protocol)
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures, as suggested below. It is also important that the managed service provider is fully aware of the SWGfL Security Policy and Acceptable Usage Policy.)
The Network Manager / Systems Manager / ICT Technician / ICT Co-ordinator is responsible for ensuring:

- **that the school's ICT infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance**
- **that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed**
- Lancsngfl is informed of issues relating to the filtering applied by the Grid
- Lancsngfl's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the *network / Virtual Learning Environment (MOODLE) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and ICT Co-ordinator for investigation / action / sanction

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**
- **they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Head teacher, ICT Co-ordinator / Class teacher for investigation / action / sanction**
- **digital communications with pupils (email / Virtual Learning Environment (MOODLE) / voice) should be on a professional level and only carried out using official school systems**.
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Senior Leader for Child Protection (DSL)

DSL should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee (comprised of pupils and parents / carers. – HT, ICT Co-ord, ICT technical, Y6 pupil(s) Parents, e-safety govr)

Members of the *E-safety committee* will assist the *E-Safety Officer* in the:

- the production / review / monitoring of the school e-safety policy / documents.
- *the production / review / monitoring of the school filtering policy*

Pupils:

- **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.** (n.b. At EYFS /KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / Moodle and information about national / local e-safety campaigns / literature.* Parents and carers will be responsible for:

- **endorsing (by signature) the Pupil Acceptable Use Policy**
- accessing the school website / Moodle/ on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems / website / MOODLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems. E.g After School Club and Guides organisation.

Policy Statements

Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- **A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site, Moodle*
- *Parents evenings*
- *Reference to the SWGfL Safe website*

Education - Extended Schools

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select / delete as appropriate)

- **A planned programme of formal e-safety training will be made available to staff. E-safety policy reviewed annually. E-Safety training accessed from local authority on INSET days. An audit of the e-safety training needs of all staff will be carried out r.**
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**
- The E-Safety Officer and COMPUTING Co-ordinator will receive regular updates through attendance at LA and other training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others..
- The E-Safety Officer and COMPUTING Co-ordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in COMPUTING / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures as suggested below. It is also important that the managed service provider is fully aware of the SWGfL Security Policy and Acceptable Usage Policy.
(nb the school should also check their Local Authority policies on these technical issues)

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities: (schools will have very different ICT infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:)

- **School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance**
- **There will be regular reviews and audits of the safety and security of school ICT systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school ICT systems• All users** at KS2 and above **will be provided with a username and password** by the ICT Co-ordinator who will keep an up to date record of users and their usernames. School may choose to use group or class log-ons and passwords for KS1 and below, but are aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access. Schools should also consider the implications of the development of Learning Platforms and home access on whole class log-ons and passwords. A school password policy template is provided in the appendix to this document)
- **The "master / administrator" passwords for the school ICT system, used by the ICT Co-ordinator must also be available to the Head teacher and Bursar kept in a secure place (eg school safe).**

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Lancsngfl.
- Any filtering issues should be reported immediately to Lancsngfl.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Co-ordinator and Head teacher an additional person should be nominated – to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. (
- Any actual / potential e-safety incident must be reported immediately to the Computing Co-ordinator and Head teacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Temporary access is given to visiting staff e.g. supply teachers to log on as supply teacher
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Computing co-ordinator can temporarily remove those sites from the filtered list for the period of study.. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption (e.g see True Crypt free ware) and secure password protected devices.**

No personal data (e.g. when full names, dates of birth, addresses are linked together - a simple class list of names would not be regarded as personal data) should be stored on any portable computer system, USB stick or any other removable media, if it is:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow pupils to use mobile phones in lessons, while others recognise their educational potential

and allow their use. This section may also be influenced by the age of thepupils. The table has been left blank for school to choose its own responses.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X					X		
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones or other camera devices				X				X
Use of hand held devices eg PDAs, PSPs	X							X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of chat rooms / facilities		X						X
Use of instant messaging		X						X
Use of social networking sites				X				X
Use of blogs		X				X		

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and pupils or parents / carers (email, chat, MOODLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

(the school should agree its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues)

(The last section of the table has been left blank for schools to decide their own responses)

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					☐
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☐
	adult material that potentially breaches the Obscene Publications Act in the UK					☐
	criminally racist material in UK					☐
	pornography				☐	
	promotion of any kind of discrimination				☐	
	promotion of racial or religious hatred				☐	
	threatening behaviour, including promotion of physical violence or mental harm				☐	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				☐	
Using school systems to run a private business					☐	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				☐	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☐	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				☐	
Creating or propagating computer viruses or other harmful files				☐	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☐	
On-line gaming (educational)	☐				
On-line gaming (non educational)				☐	
On-line gambling		☐		☐	
On-line shopping / commerce		☐			
File sharing		☐			
Use of social networking sites		☐			
Use of video broadcasting eg Youtube		☐			

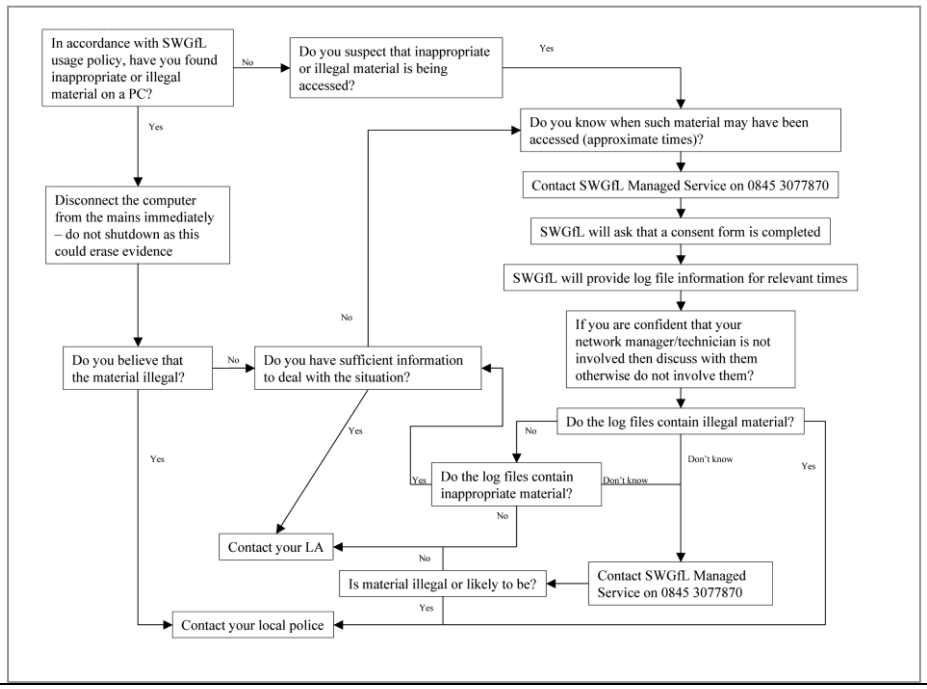
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



For SWGfL change to Lancsngfl
For technical 0845 053 0006
For content: 01257 516379

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues)

Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to ICT Co-ordinator	Refer to Head teacher/ Deputy |Head Teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	☐	☐	☐	☐					
Unauthorised use of non-educational sites during lessons	☐	☐							
Unauthorised use of mobile phone / digital camera / other handheld device	☐	☐	☐						
Unauthorised use of social networking / instant messaging / personal email	☐	☐							
Unauthorised downloading or uploading of files	☐	☐	☐		☐		☐	☐	
Allowing others to access school network by sharing username and passwords	☐	☐	☐		☐		☐	☐	
Attempting to access or accessing the	☐	☐	☐		☐		☐	☐	

school network, using another student's / pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff	☐	☐	☐		☐		☐	☐	
Corrupting or destroying the data of other users	☐	☐	☐		☐		☐	☐	☐
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☐	☐	☐		☐		☐	☐	☐
Continued infringements of the above, following previous warnings or sanctions	☐	☐	☐		☐		☐	☐	☐
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☐	☐	☐		☐		☐	☐	☐
Using proxy sites or other means to subvert the school's filtering system	☐	☐	☐		☐		☐	☐	☐
Accidentally accessing offensive or pornographic material and failing to report the incident	☐	☐	☐		☐		☐	☐	
Deliberately accessing or trying to access offensive or pornographic material	☐	☐	☐		☐		☐	☐	☐
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☐	☐	☐		☐		☐	☐	☐

Staff Actions / Sanctions

Incidents:	Refer to ICTt Co-ordinator	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	☐	☐	☐	☐	☐		☐	☐
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	☐	☐			☐	☐		
Unauthorised downloading or uploading of files	☐	☐			☐	☐		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	☐	☐			☐	☐		
Careless use of personal data eg holding or transferring data in an insecure manner	☐	☐			☐	☐		
Deliberate actions to breach data protection or network security rules		☐			☐	☐		

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		☐			☐	☐		☐
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		☐			☐	☐		☐
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications withpupils	☐	☐			☐	☐		☐
Actions which could compromise the staff member's professional standing		☐			☐	☐		☐
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		☐			☐	☐		☐
Using proxy sites or other means to subvert the school's filtering system	☐	☐			☐	☐		☐
Accidentally accessing offensive or pornographic material and failing to report the incident		☐	☐		☐	☐		☐
Deliberately accessing or trying to access offensive or pornographic material		☐	☐		☐	☐	☐	☐
Breaching copyright or licensing regulations		☐	☐		☐			
Continued infringements of the above, following previous warnings or sanctions		☐	☐					☐

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template:

- Members of the SWGfL E-Safety Group and the SWGfL E-Safety Conference Planning Group
- Avon and Somerset Police
- Somerset County Council
- Plymouth City Council
- Swindon Borough Council
- Poole Borough Council
- Bournemouth Borough Council
- North Somerset Council
- Gloucestershire County Council
- DCSF
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council
- Northern Grid for Learning
- Bracknell Forest Borough Council

- Byron Review – Children and New Technology – “Safer Children in a Digital World”

Pupil Acceptable Use Policy Agreement

From September 2015

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *pupils* will have good access to ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission (schools should amend this section in the light of their mobile phone / hand held devices policies). I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet and contact with parents.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Pupil Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, Moodle, website etc.

Name of Student / Pupil		
Group / Class		
Signed		

Staff/ Volunteer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *pupils'* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, Moodle etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / MOODLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. (See advice provided by LCC).
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school

equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without consulting ICT Co-ordinator or Head teacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Parent / Carer Acceptable Use Policy Agreement

September 2015

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *pupils* will have good access to ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above *pupil*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed		

Chorley St Mary's Catholic Primary School Filtering Policy

lancsngfl schools automatically receive a filtered broadband service. Details of the lancsngfl Internet Filtering Service and Policy can be found at lancsngfl website.

This service is intended to prevent users accessing material that would be regarded as illegal and / or inappropriate in an educational environment, as defined in the Filtering Policy. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

The Lancsngfl filtering service provides flexibility for schools to decide on their own levels of filtering security. It is possible to add to or override some of the sites filtered by Lancsngfl.

As the use of the internet becomes more widespread, access becomes available through a wider range of technologies and users become more sophisticated in their internet use, schools need to continually review their filtering and monitoring policies.

Many users are not aware of the flexibility available at a local level for schools, and other organisations, connected to Lancsngfl and its filtering service. Schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

The template document below provides a basis for a school filtering policy. Schools will however need to consider carefully the issues raised and decide:

- Whether they will adopt the Lancsngfl Filtering Policy without change
- Whether to allow flexibility for sites to be added or removed from the filtering list for your organisation.
- Whether to remove filtering controls for some internet use (eg social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used.

In the template below, sections of guidance will be written in RED, while sections shown in bold indicate those elements of the policy that are strongly recommended by SWGfL. Sections in italics indicate those elements that the school will need to consider and decide whether to include or not.

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the Lancashire Grid for Learning (LancsngfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT Co-ordinator. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
To ensure that there is a system of checks and balances and to protect those responsible, changes to the Lancsngfl / school filtering service must (schools should choose their relevant response(s):

- **be logged in change control logs**
- **be reported to a second responsible person – head teacher:**
- **be reported to and authorised by a head teacher or deputy head teacher prior to changes being made.**

All users have a responsibility to report immediately to ICT Co-ordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- *signing the AUP*
- *induction training*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

The school uses Lancsngfl LGFL Filtering Interface. The school requested devolved filtering control from the local authority which with the exception of the mandatory core categories allows school to make local changes to the default filtering policies. Any changes to the default settings require strong educational reasons.

Users may request changes to the filtering by contacting the head teacher with the url/ web address of the site they wish to use.

Some websites may be allowed or denied access. Some may be allowed for a limited period of time e.g. for the duration of the lesson.

The ICT Co-ordinator will be involved to provide checks and balances at the time of request, but could be retrospectively through inspection of records / audit of logs

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Co-ordinator who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at LancsngfL level, the responsible person ICT Co-ordinator should email **lancsngfl** with the URL.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. Monitoring will take place as follows: if required records of internet users' activity is available from schools ICT services.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *the ICT CO-ordinator*
- *E-Safety Committee on request*
- *Curriculum Committee Governors committee*
- *Local Authority on request*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.