St. Gildas' Catholic Junior School


# E-Safety Policy 2017

# CONTENTS

# Introduction

The Internet is regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail.
Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe.
This policy is designed to ensure safe internet use by pupils at school, but also to encourage safety on-line at home etc. It follows the DfE Keeping Children Safe in Education 2016 updated statutory safeguarding guidance and the July 2015 Counter-Terrorism and Security Act 'Prevent' Duty.

## 1. Core Principles of Online Safety

As stated in the updated statutory safeguarding guidance 2016, safeguarding is the responsibility of all staff who come into contact with children and their families. Online safety is a matter of safeguarding.
There should be a whole school approach to online safety including mobile technologies. Therefore online safety depends on staff, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones and tablet computers.
The updated guidance also introduces a new requirement for schools to ensure appropriate internet filters and monitoring systems are in place to protect pupils from potentially harmful and/or inappropriate online material including radicalisation. Furthermore, the guidance says it is a requirement for schools to teach pupils about safeguarding, including staying safe online and so, although schools need to put appropriate filtering and monitoring systems in place, they should be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
There is no straightforward or totally effective solution to online filtering and staff, parents and the pupils themselves must remain vigilant.

## 2. Who will write and review the policy?

It will be the responsibility of the Computing Leader to review the policy annually and alert staff to necessary updates. The updated policy should then be agreed by staff.

## 3. Why is internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, well being and to support the professional work of staff and to enhance the school's management information and business administration systems.

## 4. How will internet use enhance learning?

- The school internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate internet use and be given clear objectives for internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

## 5. How will internet access be authorised?

- The school will keep a record of all staff who are granted internet access on signing the Staff/ Governors and Volunteers Acceptable Use Agreement. The record will be kept up-to-date; for instance a member of staff may leave.
- Parents will be informed that pupils will be provided with supervised internet access (see appendix) and the school will keep a record of all pupils who are granted internet access. The record will be kept up-to-date; for instance on a pupil's access being withdrawn.
- Pupils will not be issued individual email accounts, but will be authorised to use a group/class email address under supervision.
- There is a structured approach to internet access and internet searches, with clear progression through the school. This can be seen in the Computing Curriculum planning overview, as delivered through the Switched On Computing scheme of work.

## 6. How will filtering be managed?

- The school will work in partnership with parents, TurnITon, Haringey Council, DfE and the LGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the Internet Service Provider (Virgin Broadband and LGfL) and IT support TurnITon, via the Computing Leader. (See section 15 for contact details). Parents of the children involved will be notified immediately.
- Website logs will be regularly sampled and monitored.
- The Computer Leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

# 7. How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material through the use of safety filters and monitoring. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Haringey Council can accept liability for the material accessed, or any consequences of internet access.
- The appropriateness of filters and monitoring will be informed in part by the risk assessment required by the Prevent duty.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher and Computing leader will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

# 8. Managing Content

## 8.1 How will pupils learn to evaluate internet content?

- Paragraph 68 of the safeguarding guidance now says it is a requirement for schools to teach pupils about safeguarding, including staying safe online.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Computing Leader, or directly reported to the school ICT technician at TurnITon via the TIO Support Portal.
- Schools should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
- Nominated persons (ICT technicians) will be responsible for permitting and denying additional websites as requested by colleagues.

## 8.2 How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

# 9. Communication

## 9.1 Managing e-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Whole-class or group e-mail addresses organised by the teacher should be used.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

## 9.2 On-line communications and social networking.

- Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety.
- The school will conduct annual pupil surveys about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.
- The use of online chat is not permitted in school.

## 9.3 Mobile technologies

- Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
- Parents who wish their child to bring a mobile phone to school, must first request permission from the Head teacher.
- Pupils' mobile phones will be held by the school office during the school day.
- E-readers such as Kindles etc will only be allowed after permission is granted, and such technology must not be used online whilst on the school premises.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
  Parents must agree that the school is not responsible for the upkeep and safety of any mobile phones or e-readers brought into school.

## 10. Introducing the Policy to Pupils

- Rules for Responsible ICT Use and Online Acceptable Use will be posted in all rooms where computers are used.
- A week on responsible internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Instruction on responsible and safe use should precede internet access.
- Pupils will be informed that internet use will be monitored.

## 11. Parents and E-Safety

- Parents' attention will be drawn to the School E-Safety Policy in the Home-School ICT Partnership letter, given at the start of the academic year, newsletters, the school brochure and on the school website.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- All parents will receive support information as and when available, e.g. Know It All for Parents.

## 12. Consulting with Staff and their inclusion in the E-safety Policy

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the E-Safety Policy, Acceptable ICT Use Policy, and 'What to do if' guidance, and their importance explained.
- The school's consequences for internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the 'Acceptable ICT Use Policy' before using any internet resource in school.
- Staff should be aware that internet traffic is monitored and reported by the LGfL and can be traced to the individual user. Discretion and professional conduct is essential.
- Governors, volunteers and any other community users of the school's ICT facilities must sign the acceptable user policy before being granted access.
- The school will adopt the Council's e-mail and internet user policy.
- The monitoring of internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible internet use and on the school internet policy will be provided as required.

## 13. How will complaints be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

## 14. Appendices

- Home/School ICT Partnership information for parents.
- Pupils' Code of Conduct – Rules for Responsible ICT Use.
- Pupils' Rules for Online Use.
- The Use of Digital Images and Video Policy
- The Use of Social Networking and On-line Media Policy
- Parents' Acceptable Use Agreement
- Acceptable ICT Use Policy (AIUP): All Staff, Governors and Volunteers
- 'What do we do if' Guidance

SAMPLE

Dear Parents/Carers,

**School- Home Partnership Computing and E-safety Agreement**

Nowadays most children use computer facilities including internet access as a part of everyday life. At school, use of ICT equipment including internet access is an essential part of learning, and a requirement of the National Curriculum. At St. Gildas' school, your child will regularly be given access to use a range of equipment including PCs, laptop computers, ipads, interactive whiteboards, digital cameras and the Internet. Access will always be supervised by an adult, with the greatest consideration given to safety.

Although there are concerns about children having access to inappropriate material via the Internet, the school takes a range of measures to minimise these risks. A filtering system, through the LGFL (London Grid For Learning) is in operation, which restricts access to inappropriate materials, and this is supplemented by an Internet safety, 'esafety' programme for all children, which teaches pupils about safeguarding including staying safe online. Pupils are taught about the safe and appropriate behaviours to adopt when using the Internet, email and other technologies, the risks associated, and what to do when encountering risks.

We have recently rewritten our e-safety and computing policies to conform to the most current standards of practice, ensuring that safeguarding of children is at the heart of all that we do. Copies of the following policies are included with this letter.

- St. Gildas' ICT Code of Conduct; Rules for Responsible ICT use for pupils
- Pupil Online Acceptable Use Agreement
- Use of Digital Images and Video Policy
- Use of Social Networking and On-Line Media Policy
- Parents' Acceptable Use Agreement

Before granting access to school equipment, both pupils and their parents/carers will be asked to sign to show that the e-safety rules have been understood and agreed. Signed agreements will be kept at the school office within pupil's school files.

We would be grateful if you would return the signed enclosed documents, to the school office by Monday 11th September.

All of the attached information, and our full E-safety Policy is available to read and download, alongside other helpful internet safety information, within the e-safety section and policy section of the school website, which can be found at www.stgildas.co.uk .

Yours sincerely,

G. Hood
Headteacher

## St. Gildas' ICT Code of Conduct:

## Rules for Responsible ICT Use for Pupils

- I will only use ICT equipment and access the system with adult permission and supervision.
- I will not access other people's files.
- I will use the computers and Ipads for instructed schoolwork and homework only.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I understand that the school may check my computer files and may monitor the internet sites I visit.

I have read and understand these rules and agree to them.

Signed: _____ (Pupil) Date: _____

Printed name: _____

## Pupil Online Acceptable Use Agreement

***This agreement will help keep me safe and help me to be fair to others.***

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

**I have read and understood this agreement.**

**I know who are my trusted adults are and agree to the above.**

Signed: _____ Date: _____

## The Use of Digital Images and Video Policy

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following 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.

Only images of pupils in suitable dress are used.

Staff are not allowed to take photographs or videos on their personal equipment.

---

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

- Your child being photographed (by the class teacher or teaching assistant) 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.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your 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, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

## The Use of Social Networking and On-line Media Policy

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common Courtesy**
- **Common Decency**
- **Common Sense**

*How do we show common courtesy online?*

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

*How do we show common decency online?*

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

*How do we show common sense online?*

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
*(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)*

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

## Parents' Acceptable Use Agreement

**Internet and ICT:** As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

**Use of digital images, photography and video:** I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

**Social networking and media sites:** I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

**My daughter / son name(s):** _____

**Parent / guardian signature:** _____

**Date:** ___/___/___

| | | |
|---|---|---|
| | **Name of School** | **St. Gildas' Catholic Junior School** |
| | **AUP review Date** | **September 2017** |
| | **Date of next Review** | **September 2018** |
| | **Who reviewed this AUP?** | **Miss Ashworth** |

## Acceptable ICT Use Policy (AIUP): All Staff, Governors and Volunteers

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, social networking tools, school website, equipment and systems.

St. Gildas' regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone and will not record it in place where it could be easily discovered (such as the back page of a diary).
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to*.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: LGfL StaffMail
- I will only use the approved LGfl StaffMail, and school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head Teacher and Computing Leader.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's network security updates.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school and will only use in staff areas.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within school.
- I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc., will not identify students by name, or other personal information.
- I will use the school's online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the school approved Cisco system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the Safeguarding Lead if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the Safeguarding Lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head Teacher and Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

## Acceptable ICT Use Policy (AIUP): Agreement Form

## All Staff, Governors and Volunteers

**User Signature**

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

**Authorised Signature (Head Teacher / Deputy)**

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date.....

Full Name ..... (printed)

| | | |
|---|---|---|
| | **Name of School** | **St. Gildas' Catholic Junior School** |
| | **AUP review Date** | **September 2017** |
| | **Date of next Review** | **September 2018** |
| | **Who reviewed this AUP?** | **Miss Ashworth** |

## Guidance: What do we do if?

**An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.**

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e-safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the Computing Leader/ Trainer, or school technicians directly and ensure the site is filtered (TIO Support Portal).
4. Inform Haringey LA.

**An inappropriate website is accessed <u>intentionally</u> by a child.**

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be. (TurnITon)
4. Inform Haringey LA.

**An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT providers, this could include LGfL and your technical support provider to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or CEOP and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

**A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.

7. Inform the police if necessary.
8. Inform the LA e-safety officer.

**Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.**

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.

**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child**

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

**Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.**

Do you have a cyberbullying or digital safety concern?

helpline@saferinternet.org.uk

0844 381 4772

**Hours of operation are Monday to Friday, 10am to 4pm. The Helpline can be emailed at any time, and these will be responded to during our normal working hours.**

# TOP TIPS

- **Talk to your child about what they're up to online**. Be a part of their online life; involve the whole family and show an interest. Find out what sites they visit and what they love about them, if they know you understand they are more likely to come to you if they have any problems.
- **Watch Thinkuknow films and cartoons with your child**. The **Thinkuknow site** has films, games and advice for children from five all the way to 16.
- **Encourage your child to go online and explore!** There is a wealth of age-appropriate sites online for your children. Encourage them to use sites which are fun, educational and that will help them to develop online skills.
- **Keep up-to-date with your child's development online**. Children grow up fast and they will be growing in confidence and learning new skills daily. It's important that as your child learns more, so do you.
- **Set boundaries in the online world just as you would in the real world**. Think about what they might see, what they share, who they talk to and how long they spend online. It is important to discuss boundaries at a young age to develop the tools and skills children need to enjoy their time online.
- **Keep all equipment that connects to the internet in a family space**. For children of this age, it is important to keep internet use in family areas so you can see the sites your child is using and be there for them if they stumble across something they don't want to see.
- **Know what connects to the internet and how**. Nowadays even the TV connects to the internet. Make sure you're aware of which devices that your child uses connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection, or a neighbour's wifi? This will affect whether the safety setting you set are being applied.
- **Use parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones**. Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops. They are not the answer to your child's online safety, but they are a good start and they are not as difficult to install as you might think. Service providers are working hard to make them simple, effective and user friendly. **Find your service provider and learn how to set your controls**

**e-Safety Links**

*Use Websites that provide information and guidance on e-safety.*

Think U Know
Recommended e-safety website
*http://www.thinkuknow.com/*

Child Exploitation And Online Protection
http://ceop.police.uk/

Advice, help and Report centre
*http://www.ceop.police.uk/safety-centre/*

http://www.childnet.com/
Childnet International, a non-profit organisation working with others to help make the internet a great and safe place for children.

Facebook Safety Centre
https://en-gb.facebook.com/safety/

By TIME –tech a list of social networking sites for children under 13
http://techland.time.com/2012/05/24/the-best-social-networks-for-kids-under-13/

10 worst password ideas
http://techland.time.com/2013/08/08/google-reveals-the-10-worst-password-ideas/?iid=obinsite

## 15. Web-based Resources For Schools

**KidSmart**
http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents

**Childnet International**
http://www.childnet-int.org/
Guidance for parents, schools and pupils

**Grid Club**
http://www.gridclub.com/
On-line activities for Key Stage 2 pupils to teach e-safety.

**London Grid for Learning**

http://www.lgfl.net/lgfl/sections/safety/esafety/menu/
e-safety materials (posters, guidance etc.)

**DfES Anti-Bullying Advice**
http://www.dfes.gov.uk/bullying/

**Internet Watch Foundation**
www.iwf.org.uk
Invites users to report illegal Websites

**Think U Know**
www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

## For Parents

**Kids Smart**
http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

**Childnet International**
http://www.childnet-int.org/
“Know It All” CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

## 15. Useful contact details:

TurnITon- Use TIO Support Portal
London Grid for Learning (LGfL) Support Team - Telephone: 020 8255 555
Email support@lgfl.org.uk

## 16. Notes on the Legal Framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.
The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.
Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.
A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.
Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The Rules for Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.
In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day / week / month. Though this is not user specific it does allow a degree of monitoring to be conducted. All schools are also able to monitor school e-mail.
Cyber-stalking & Harassment (http://wiredsafety.org/gb/stalking/index.html)
Under Section 1 of the Malicious Communications Act 1998 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5000. As the Malicious Communications Offence is more wide-ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyber-stalking however there will be more than one offensive or threatening letter or telephone call and therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from Harassment Act 1997 the court can make a Restraining Order preventing them from contacting their victim again. Breach of a Restraining Order is punishable with up to five years' imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-stalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997 which is punishable with up to five years' imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-stalking etc. is racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or 32(1)(b) of the Crime and Disorder Act 1998. If convicted offenders could face up to 7 years' imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.

## 17. Glossary of Terms

Blog – Short for Web Log, an online diary

DFE - Department for Education

Podcast – a downloadable sound-recording that can be played on computers and MP3 players

LGfL – London Grid for Learning, which provides Internet access and associated managed services to all schools in London

Social Networking – websites that allow people to have “pages” that allow them to share pictures, video and sound and information about themselves with online friends

Video Blogging – online videos that can be uploaded via a web cam

Web 2 Technologies – a collection of online web services that are based around communicating/sharing information