# E Safety Policy

YEALMPTON PRIMARY SCHOOL

## E-Safety Policy

### 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. This e-safety policy should help to ensure safe and appropriate use. 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 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 demonstrates through the e- safety Policy and related Security Password Policy and Personal Data Policy  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.

**Monitoring**

The E- Safety coordinator (Computing Subject Leader) will:

- Review the E Safety policy annually ; or more regularly in the light of any significant new developments in the use of technologies, new threats to e- safety or incidents that have taken place
- Report any serious e-safety incidents that take place to the Local Authority, Head teacher, LA Safeguarding Officer and Police Commissioner's Office
- Monitor the impact of the policy using:
  - pupils (e.g. Ofsted "Tell-us" survey / CEOP Think U know survey)
  - parents / carers
  - staff

**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.

At Yealmpton School the pupils currently have access to a number of websites.

The teachers will act on any information regarding inappropriate internet home use and liaise with parents and the Head/ Deputy teacher to safeguard pupils. 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.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular meetings with ICC ICT technicians

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members who are the E- safety Link governor/ 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 National Governors Association / SWGfL
- Participation in school training / information sessions for staff or parents

**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 E-Safety Co-ordinator
- The Head teacher is responsible for ensuring that the E-Safety Coordinator 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 and another member of the Senior Leadership Team 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 relevant Local Authority HR / disciplinary procedures)

**E- Safety Co-ordinator/ICC ICT Department:**

- Liaises with the E-Safety link governor and keeps the Governors informed of current issues.
- 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
- Provides training and advice for staff
- Liaises with ICC head of e-safety
- Liaises with school ICT technical staff (ICC ICT department)
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reports regularly to Senior Leadership Team any issues regarding Safeguarding and E-safety
- Ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensures 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
- Ensures that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Ensures that SWGfL is informed of issues relating to the filtering applied by the Grid
- Ensures the SWGfL's filtering policy is applied. The SWGfL Policy is updated on a regular basis and its implementation is not the sole responsibility of any single person. The Computing Subject Leader ensures that the SWGfL filtering policy is applied in conjunction with the Headteacher and school administrator.
- 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
- Ensures that monitoring software / systems are implemented and updated as agreed in school policies

**Teaching and Support Staff**:

It is essential that all staff receive e-safety training and training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly
- 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 policy.
- This E-safety policy and its updates will be discussed by staff INSET
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

**Staff responsibilities will include to:**

- Have an up to date awareness of e-safety matters and of the current school e-safety policy
- Read, understand and sign  the school Staff Acceptable Use Policy (AUP)
- Report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action
- Ensure any digital communications with pupils (email / Virtual  Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- Ensure e-safety issues are embedded in all aspects of the curriculum and other school activities
- Ensure pupils understand and follow the school e-safety and acceptable use policy
- Ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations where appropriate
- Monitor Computing activity in lessons, extra curricular and extended school activities
- Be 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
- Check suitability of sites in lessons where internet use is pre-planned and guide  pupils to sites checked for their suitability of use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**Designated Child Protection officer:**

- Trained in e-safety issues
- 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

**Pupils:**

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

- A planned e-safety programme should be provided and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- 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
- 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.

**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.

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

- Newsletters
- School website signposting
- Parents evenings when appropriate
- Circulating  Child net 'Think You Know ' or 'Know it all'  resources to all new families or any other available resources that support the aims of the e- safety policy

Parents/Carers will be encouraged to support e- safety:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website / VLE / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

**Community Users:**
Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

### Technical – infrastructure/ equipment, filtering and monitoring

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:

### Users Log ons

- All users at KS2 will be provided with a username and password by the Computing Subject Leader/ICC technicians informing class teachers. ICC technicians will keep an up to date record of users and their usernames. Users will be required to change their password every term.
- All users at Foundation and KS1 to use Key Stage logon. 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
- The school will adopt a school password policy prior to the introduction of the use of website user log- ons
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (Administrator ) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. 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
- All users will have clearly defined access rights to school ICT systems. Detail of the access rights available to groups of users will be recorded by the ICT Subject Leader. This will be reviewed annually by the E-safety committee

### ICT Systems

- Servers , wireless systems and cabling must be securely located and physical access restricted
- 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 an annual review and audit of the safety and security of the school IT systems
- The school maintains and supports the managed filtering service
- In the event of the ICC ICT technicians needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher (or other nominated senior leader).
- Any filtering issues should be reported immediately

- Requests from staff for sites to be removed from the filtered list will be considered by the Computing Subject Leader, ICC ICT technicians, Head teacher and Governor Committee. If the request is agreed, this action will be recorded.
- Remote management tools are used by staff to control workstations and view user's activity. This may occur through ICC ICT department
- Any actual / potential e-safety incident must be reported to the Computing Subject Leader / 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
- The school infrastructure and individual workstations are protected by up to date virus software
- The ICC ICT department with the approval of the Head teacher is responsible for installing programmes on school workstations / portable devices and this is forbidden for other staff members
- The school has ensured that the use of removable media and portable workstations (laptops) are encrypted. Personal data will **not** be taken off the school site unless safely encrypted or otherwise secured. (See School Personal Data Policy)
- The school administrator securely stores all school data using a terminal server offsite
- The provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system is organised by the Computing Subject Leader with approval of the Head teacher
- Teaching staff need to seek approval by the Computing Coordinator ( with approval of the Head teacher) regarding the downloading of executable files by users
- Teaching Staff predominantly use portable laptops for work use and keep personal use to a minimum and it has been agreed that their family members are not allowed on laptops and other portable devices that may be used out of school
- Teaching Staff are permitted to use removable media, CDs / DVDs by users on school workstations / portable devices off site for the preparation of lessons and if the Computing Subject Leader has confirmed the site licence permits this

## 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 students / 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 students / 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.
- Staff ensure that they have researched and prepared suitable sites so pupils are directed to research topics (e.g racism, drugs, and discrimination) in sites that are not blocked. Pupils will not be permitted to research topics unsupervised and carry out searches that would normally result in internet searches being blocked.
- 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 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 pupil's 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.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- 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 e.g. 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 or cause embarrassment .
- 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 (This forms part of the AUP signed by parents or carers at the start of the child's attendance at Yealmpton Primary and lasts for the duration of their stay (see Parents / Carers AUP Agreement in the appendix)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

### 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.
- Refer to School Data Protection Policy

**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 encrypted 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 and secure password protected devices such as school encrypted memory sticks

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected ( November 2009 )
- The removal of personal or confidential information will only be allowed when all files encrypted.
- All school laptops for take home by teachers are encrypted and encrypted memory sticks are used to transfer personal or confidential information.(November 2009)
- 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 √
- The removal of personal data must be kept to a minimum and data storage on removal media will only be allowed using an encrypted memory stick ( November 2009 )

**Communication Technologies**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:
The following technologies are allowed supervised by a member of staff:

| | **Staff & other adults** | | | | **Students / 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 | | √ | | | | √ | | |
| Use of mobile phones in lessons | | | | √ | | | | √ |
| Use of mobile phones in social time | √ | | | | | | | √ |
| Taking photos on mobile phones or other camera devices | | | | √ | | | | √ |
| Use of hand held devices eg PDAs, PSPs | | | √ | | | | √ | |
| Use of personal email addresses in school, or on school network | √ | | | | | √ | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Use of school email for personal emails | | | | √ | | | | √ |
| Use of chat rooms / facilities | | | | √ | | | | √ |
| Use of instant messaging | | | | √ | | | | √ |
| Use of public social networking sites * | | | √ | | | √ | | |
| Use of blogs | | √ | | | | √ | | |

* Social networking sites maybe considered by teachers but all use must be supervised, for example there is a new educational social networking site launched.

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

- The official school email service account may be regarded as safe and secure and is monitored. Staff and governors should therefore use only the school email service to communicate with others when in school, or when working away from school (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Head teacher 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, staff and other colleagues, staff and governors (email, chat, VLE etc) must be professional in tone and content.
- Public chat / social networking programmes must not be used for school communications.
- Pupils will 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.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**Unsuitable / Inappropriate Activities**

Some internet activity e.g. 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 those 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. Access to the highlighted sites may be appropriate at times i.e. educational games, online shopping by office staff for resources/stock and social networking sites for educational purposes to teach about e- safety.

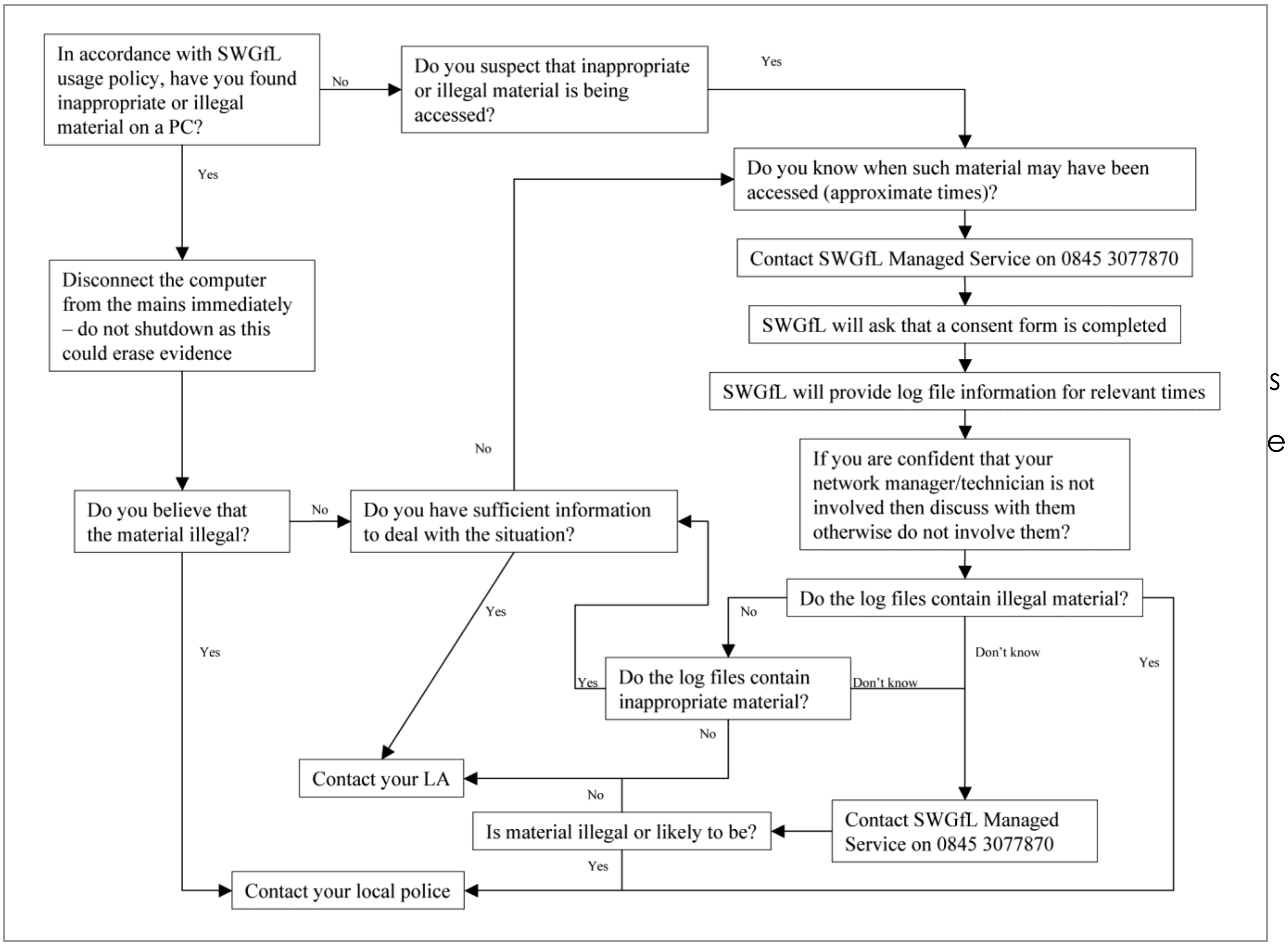
| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals 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 You tube** | | | □ | | |

**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 i.e.

- 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.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
No
Yes
Don't know
Yes
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

s

e

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:

**Pupils** **Actions / Sanctions**

| Incidents: | Refer to class teacher | Refer to Deputy Headteacher | Refer to Head teacher | Refer to Police | Refer to technical | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | □ | | □ | | □ | | | |

Staff Actions / Sanctions

| Incidents: | Refer to line manager | Refer to Head teacher | RRefer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for | 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).** | | □ | □ | □ | | | | |