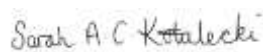





***“Let your light shine” Matthew 5:16***

Everyone is encouraged to shine by encompassing our values of respect, trust, honesty, thankfulness and resilience. Enabling us to grow, learn and achieve together.

# E-Safety Policy 2023

	Date	Signature
Discussed at Staff Meeting	17.05.23	
FGB:	11.07.23	

Responsibility of Full Governing Body

Next Review Date: May 2024

### **Vision Statement**

The School's Christian Vision Statement "Let your light shine" is our central vision. Everyone is encouraged to shine through living out our values of trust, honesty, thankfulness, respect and resilience. Enabling us to grow, learn and achieve together

## INTRODUCTION & AIM

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 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 to promote effective learning. Children and young people are spending an increasing amount of their time involved in online activities but 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 a wider duty of care to which all who work in schools are bound. A school e-safety policy should help 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 head teacher and governors to senior leaders, classroom teachers, support staff, members of the community and the pupils themselves.

The use of these exciting, innovative and ever-changing tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside 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 (this is of particular concern under GDPR legislation);
- The risk of being subjected to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal images without an individual's knowledge or consent;
- Inappropriate communication/contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable or age-inappropriate video content or gaming;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music, gaming or video files;
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person, and possibly their mental health.

Many of these risks reflect situations in the 'real world' and it is essential that this policy is used in conjunction with other school safeguarding policies, e.g. '**Anti-Bullying Policy**', '**Acceptable Use Policy**' and '**Child Protection & Safeguarding Policy**'.

As with all other risks, it is impossible to eliminate these risks completely or to be monitoring all of the children's online activity, particularly outside of school. It is therefore essential, through good educational provision and building pupils' resilience to the risks to which they may be exposed, that they have the confidence and skills to deal with these risks independently.

Cold Harbour CE Primary School strives to provide the necessary safeguards to help ensure that everything is done which is reasonably expected of them to manage and reduce the risks. This E-Safety Policy explains how we intend to do this, while addressing wider educational issues in order to help pupils and their parents/carers be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use. Indeed, upskilling parents and carers can play a key role in reducing the potential risks children are exposed to whilst online.

## SCOPE OF THE POLICY

The E-Safety Policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school computing 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 impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other e-safety incidents, which may take place out of school.

The school will deal with such incidents within guidelines detailed in the '**Relationships and Behaviour Policy**' and will, where known, always inform parents/carers of the inappropriate action that has taken place and the penalty imposed.

## PRINCIPLES OF POLICY

E-Safety is an integral part of our operations at Cold Harbour CE Primary School. It is an area where great importance is placed. We aim to fulfil our duty of promoting e-safety through the following areas:

### ***PUPIL EDUCATION:***

The key aim is to educate the pupils to take a responsible approach with IT and to know how to keep themselves safe whilst online. The education of pupils in e-safety is therefore an essential part of Cold Harbour'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:

- Planned, age-specific e-safety lesson(s) will be delivered to each year group as a stand alone lesson each half term through our ICT curriculum. This will be followed up by work in other sessions, e.g. PSHE, and will be revisited regularly. This work will cover the use of new technologies and potential online risks, both in and out of school.
- Key e-safety messages will be reinforced as appropriate during assemblies, e.g. during anti-bullying events & through visits.
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and will be guided to validate the accuracy of information.
- Pupils should be helped to understand the rules of the 'Acceptable Use Policy' (AUP) agreement (on screen and on paper). They will be encouraged to adopt safe and responsible use of computing, the internet and mobile devices both within and outside of school.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using materials accessed on the internet.
- Staff will act as good role models in their use of computing, the internet and mobile devices.

### ***PARENT/CARER EDUCATION:***

Many parents and carers have only a limited understanding of e-safety risks and issues (and even the level of online exposure), yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online 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 what to do about it. "There is a generational divide" (Byron Report). Cold Harbour CE Primary School will therefore seek to provide information and awareness to parents through:

- Newsletters
- Posts on Class Dojo and ParentMailPMX
- Parent workshops

- The School website
- The AUP

### **STAFF EDUCATION:**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in the '**E-Safety Policy**' and '**Acceptable Use Policy**'. Training will be offered as follows:

- E-Safety training will be built into INSET schedules as appropriate.
- E-Safety updates will be provided as necessary through CPD sessions and weekly briefings.
- All staff will sign the AUP agreement and will be bound by the conditions outlined. • All new staff (including students) should receive an e-safety 'induction talk' ensuring that they fully understand the contents of the '**E-Safety Policy**' and '**Acceptable Use Policy**'.
- The e-safety leader will disseminate any relevant information from updates/training accessed.
- The e-safety policy and other related policies will be updated in consultation with staff.
- The e-safety leader will provide advice, guidance and training to individuals as required/requested.

### **GOVERNOR EDUCATION:**

Governors should take part in e-safety training and awareness sessions as appropriate. This is of particular importance to any partner governor teams with specific responsibility for safeguarding. This training may be offered in a number of ways including:

- Attendance at training provided by an external agency/organisation.
- Participation at a school based training event.
- Accessing information provided online, e.g. web based updates or emails.

### **TECHNICAL:**

Cold Harbour CE Primary School, along with the relevant IT technical support team, will be responsible for ensuring that the school infrastructure/network is as safe and secure as reasonably possible and that policies and procedures, outlined in this policy and other related policies, are implemented. It will also ensure that the relevant personnel, e.g. e safety leader, will be effective in carrying out their e-safety responsibilities.

School computing systems will be managed in ways that ensure Cold Harbour CE Primary School meets any e-safety technical requirements recommended to schools. There will be regular reviews and audits of the safety and security of school computing systems servers, wireless systems and cabling will be securely located and physical access to server areas will be restricted.

All users will have clearly defined access rights to the school computing systems. Details of the access rights will be reviewed annually by the IT technical support team in consultation with the senior leadership team. This review will be confirmed to the governing body committee responsible for e-safety.

All users will be provided with a user name and password by the IT technical support team. Users will be reminded about the need to keep their password confidential and to log off when they leave a machine unattended. Children will be issued with a log in as their use of the network will be monitored. Both pupils and staff should only ever access the school network through their individual login details. Their password can be changed as required by informing the IT technical support team.

The administrator passwords for the school computing systems, should only be used by the IT technical support team. This information must be stored securely, e.g. the school safe.

Users are responsible for the security of their username and password. They must not allow others users to access the systems using their login detail and must immediately report any suspicion or evidence that there has been a breach of security. The implications of GDPR legislation should be considered at all times.

Cold Harbour CE Primary School adopts the filtering and monitoring systems provided as part of the local service agreement. All users should be regularly reminded about the monitoring and filtering which is in place on the systems and networks.

In the event that the IT technical support team (or any other person) requires the filtering and monitoring systems to be switched off, this must be authorised and agreed by the head teacher and/or deputy head teacher. Requests from staff for sites to be removed from the filtered list will be considered by the IT technical support team in consultation with the senior leadership team.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

An '**Acceptable Use Policy**' outlines the terms of agreement, which users of the school computing systems have to adhere to. This policy outlines the extent to which school equipment may be used for personal reasons outside of school. It also details rules on removing or installing additional software as well as the use of removable media, e.g. memory sticks.

The school infrastructure and individual workstations are protected by up-to-date virus protection software.

## ***CURRICULUM:***

E-safety is of paramount significance at Cold Harbour CE Primary School and staff are encouraged to reinforce e-safety messages in the use of computing across the curriculum by noting the following points:

- 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, e.g. by using search engines, staff should be vigilant in monitoring the content of the websites being visited.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT technical support team can temporarily remove these sites from the filtered list for a period of study.
- 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:***

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images 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 posting digital images on the internet. These images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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 ensure that these are transferred to a secure area on the school network/encrypted laptop immediately on return to school (if from an off-site visit) and before the camera is removed from site (if taken on-site). Staff are encouraged to use school equipment to take digital images and should not use own devices unless given prior permission by the head teacher. Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute.

Any images collected shall only be shared, used, published or distributed in a way that is agreed by parents, e.g. staff will show compliance with the consent form signed by every parent in the school. Images published on the school website will be selected carefully and will comply with good practice guidance, e.g. names shall not be published with images and all pictures will be within GDPR legislation.

### **DATA PROTECTION:**

Personal data will be recorded, processed, transferred and made available according to GDPR legislation 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 subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- Take care at all times to ensure the safekeeping 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 password protected services.

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

- the data must be password protected and/or encrypted.
- the device must be password protected wherever possible (many memory sticks 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 once its use is complete or upon termination of employment from Cold Harbour CE Primary School.

## COMMUNICATIONS:

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

Communication Technologies	STAFF & OTHER ADULTS				PUPILS			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phone may be brought into 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			X					X
Use of hand held devices e.g. PDAs, iPads	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 room facilities		X				X	X	
Use of instant messaging		X				X	X	
Use of social networking sites		X	X					X
Use of blogs	X					X	X	

\* But must be agreed previously and be locked away by the school office until the end of the day

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

- The official school email service (Google mail) is regarded as safe and secure.
- Staff email addresses can be shared and used to correspond with parents. However, communication must be kept strictly professional and written in the same tone that would constitute professional practice between parents and teachers.
- Communication with children via email is prohibited.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the e-safety coordinator and/or head teacher/deputy head teacher, 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 parents must be professional in tone and content. These communications may only take place on monitored school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Whole class or group email addresses will be provided as requested. Requests for individual pupil email addresses will be considered by the IT technical support team and/or the head teacher.
- Personal information should not be stored on the school website and only official email addresses should be used to identify members of staff.



## ***UNSUITABLE ACTIVITIES:***

Cold Harbour CE Primary School considers the activities listed below to be inappropriate in a school context and that users should not engage in these activities in or outside of school.

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, e.g. 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
- Pornography
- Promotion of any kind of discrimination contrary to the Equality Act 2010
- 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

Users of school computing systems may not:

- Use school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Cold Harbour CE Primary School
- Upload, download or transmit commercial software or any other copyright materials belonging to third parties, without the necessary licensing permissions
- Reveal or publicise confidential or proprietary information, e.g. financial/personal information, databases, computer/network access codes and passwords
- Create or propagate computer viruses or other harmful files
- Carry out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet
- Participate in non-educational online gaming or gambling

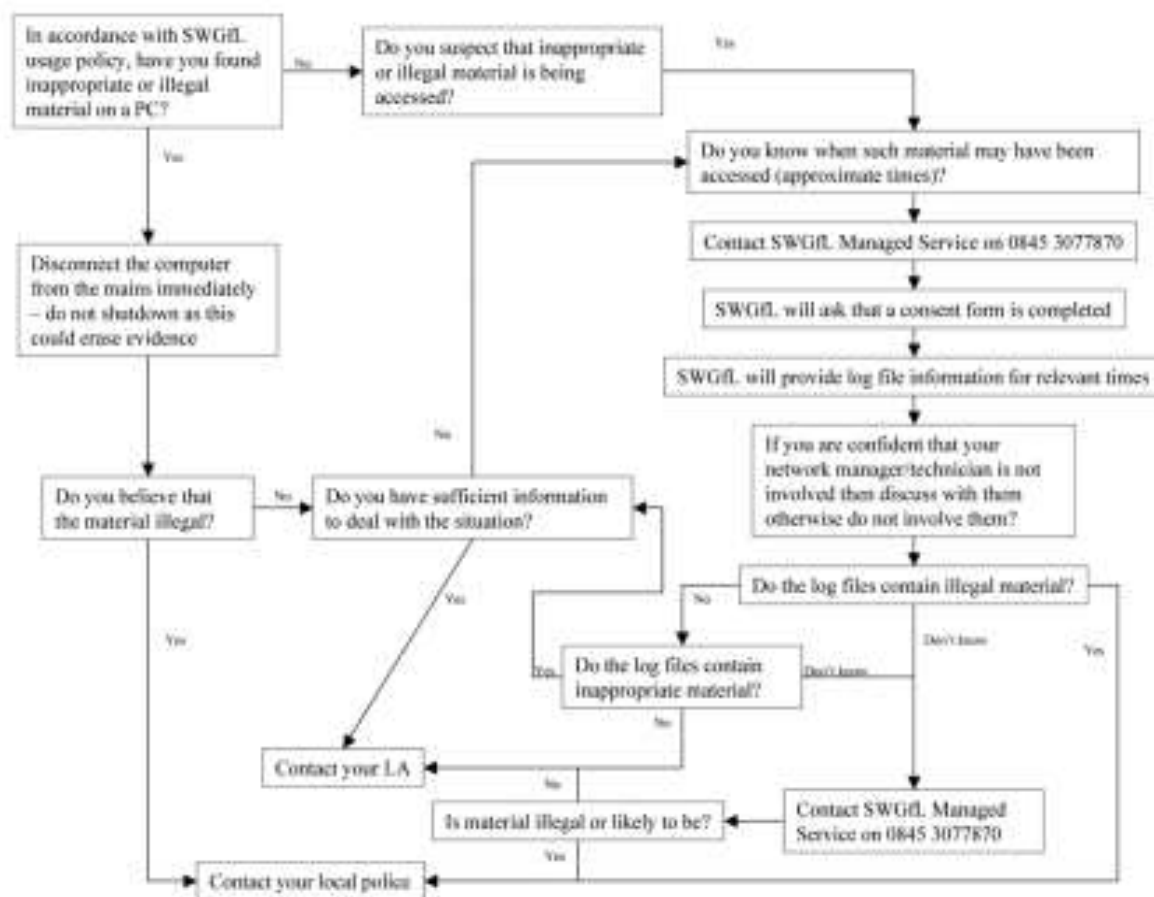
## ***RESPONDING TO INCIDENTS OF MISUSE:***

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

If any apparent or actual misuse appears to involve illegal activity, e.g.:

- 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 (available from [www.swgfl.org.uk/Staying-Safe](http://www.swgfl.org.uk/Staying-Safe) and shown below) 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.



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 disciplinary procedures.

## **ROLES AND RESPONSIBILITIES:**

### **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 may be delegated to the e-safety co-ordinators.
- The head teacher/senior leaders are responsible for ensuring the e-safety leader and other relevant staff receive suitable CPD to enable them to carry out their roles and to train other colleagues as relevant.
- The head teacher/senior leaders will ensure systems are in place for monitoring and supporting those who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring duties.
- The senior leadership team will receive regular monitoring reports.

- 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.

#### **E-Safety Leader:**

- Attend the relevant Governing Body committee meetings where responsibility is taken for e-safety as required.
- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing school e-safety procedures.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff.
- Liaise with the Local Authority and IT technical support team as appropriate, ensuring relevant information is gathered to show compliance with audit requirements.
- Receive reports of e-safety incidents and log any breaches identified through in house monitoring systems.
- Regularly meet the governor responsible for e-safety to discuss current issues, review incident logs and filtering procedures.

#### **IT Technical Support Team:**

The IT technical support team is responsible for ensuring:

- That the school's computing infrastructure is secure and is not open to misuse or a malicious attack.
- That the school meets the e-safety technical requirements recommended to schools.
- That users may only access the school's networks through clearly defined user accounts, which are securely protected.
- That the school's virus protection software and back-up systems are up-to-date and in operation at all times.

#### **Teaching and Support Staff:**

Teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current 'E-Safety Policy' and procedures.
- They have read and understood the 'Acceptable Use Policy' (AUP) and agreement.
- They report any suspected misuse or problem (including accidental navigation to inappropriate websites) to the e-safety co-leader and/or head teacher for investigation.
- Digital communications with pupils are on a professional level and through the agreed areas, e.g. Dojo.
- E-safety issues are effectively embedded throughout their teaching and curriculum delivery.
- Pupils understand and follow the school rules regarding acceptable use of Computing.
- That they monitor computing activity in lessons, extra-curricular and extended school activities.
- That they are aware of any safety issues related to the use of mobile phones, cameras and hand held devices and they are aware of the school's policy of usage with regard to these devices.
- Remind any members of staff who have an e-safety concern, they should log it on CPOMS using information and speak to the DSL and IT Lead where appropriate.

#### **Designated Safeguarding Lead:**

The DSL should be trained in e-safety issues and be made aware of the potential for serious child protection issues, which may arise from:

- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

**Governing Body/Partner Governor Team responsible for ESafety:**

Delegated members of the FGB will assist the e-safety leader with:

- The production, review and monitoring of e-safety policy and documents.
- The review and monitoring of the school filtering and monitoring systems.

**Pupils:**

Pupils are responsible for:

- Using the school computing systems in accordance with the 'Acceptable Use Policy' agreement.
- Developing a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Ensuring that they do not bring to school or attempt to connect to the school network and computing devices, which they are not authorised to do so, e.g. mobile phones.
- Adopting good e-safety practices when using digital technologies in or out of school.

**Parents/Carers:**

Parents/carers play a crucial role in ensuring that their children understand the need to use Computing 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 computing than their children.

Cold Harbour CE Primary School will therefore take every opportunity to help parents understand these issues so that they can be responsible for:

- *Endorsing (by signature) the 'Pupil AUP Agreement'*
- Supporting the school procedures to ensure e-safety at all times.

**MONITORING & REVIEW:**

Monitoring and review of the 'E-Safety Policy' should include consultation with the following groups of people:

- E-safety leader
- Head teacher and/or other senior leaders
- Teachers
- Support staff
- Computing systems manager
- Governors
- Parents and carers
- Pupils

The E-Safety Leader meets with an appointed E-Safety group periodically and will review policy and procedures through that forum.